TP-LINK®

24口千兆+4口万兆可堆叠
三层网管交换机

T3700G-28TQ

用户手册

REV1.0.2
1910040540

声明

目录

第1章 用户手册简介

本手册旨在帮助您正确使用这款交换机。手册中包括对交换机性能特征的描述以及配置交换机的详细说明。请在操作交换机前，详细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指T3700G-28TQ 24口千兆+4口万兆可堆叠三层网管交换机，下面简称为T3700G-28TQ。
- 用 **>>** 符号表示配置页面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**。
- 正文中出现的<>尖括号标记的文字，表示Web页面的按钮名称，如<确定>。
- 正文中出现的**加粗**标记的文字，表示交换机的各个功能的名称，如**端口配置**页面。
- 正文中出现的“”双引号标记的文字，表示配置页面上出现的名词，如“IP地址”。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.3 章节安排

章节	章节说明
第1章 用户手册简介	帮助您快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。
第2章 产品介绍	介绍本产品的特性、应用以及外观。
第3章 配置指南	介绍如何登录交换机的Web页面，并简要介绍配置注意事项。

章节	章节说明
第4章 系统管理	本模块主要用于配置交换机的系统属性，主要介绍了： ● 系统信息：配置交换机的描述、时间和网络参数。 ● 用户管理：配置登录交换机Web页面的用户的访问权限和身份。 ● 系统工具：集中对交换机的配置文件进行管理。 ● 安全管理：安全管理：针对不同的登录方式，增强用户管理交换机的安全性。包括安全配置、SSL配置和SSH配置。
第5章 堆叠功能	本模块主要用于配置网络中多台交换机进行堆叠。
第6章 二层交换	本模块主要用于配置交换机的基本功能，主要介绍了： ● 端口管理：配置交换机端口的基本属性包括端口配置、端口镜像、端口安全、端口隔离和环路监测。 ● 汇聚管理：配置端口汇聚组。汇聚是将交换机的多个物理端口聚合在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。 ● 流量统计：统计流经各个端口的数据信息。 ● 地址表管理：配置交换机的地址表。地址表是交换机实现报文快速转发的基础。
第7章 VLAN	VLAN主要用于隔离广播域，通过划分虚拟工作中来简化网络管理，主要介绍了： ● 802.1Q VLAN：划分基于端口的VLAN，是协议VLAN的基础。 ● MAC VLAN：配置基于MAC地址的VLAN，使指定MAC的设备接入网络时，其数据均在MAC VLAN中转发。 ● 协议VLAN：从应用层划分VLAN，使某些特殊网络数据只能在指定VLAN中传输。 ● VLAN VPN：通过VLAN映射将私网报文的VLAN Tag映射到公网VLAN Tag，并在公网VLAN传输报文。 ● GVRP：通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。 ● Private VLAN：通过建立Private VLAN，上层设备只需识别少量的primary VLAN，从而节省上层设备的VLAN资源。
第8章 生成树	生成树主要用于在局域网中消除环路。本模块主要用于配置交换机的生成树功能，主要介绍了： ● 基本配置：配置和查看交换机生成树功能的全局属性。 ● 端口配置：配置端口的CIST参数。 ● MSTP实例：配置MSTP实例。 ● 安全配置：配置保护功能，以防止生成树网络中的设备遭受恶意攻击。

章节	章节说明
第9章 组播管理	本模块主要用于配置交换机的组播管理功能，主要介绍了： ● IGMP侦听：配置IGMP侦听的全局参数、端口属性、VLAN参数和组播VLAN。IGMP侦听可以有效抑制组播数据在网络中扩散。 ● 组播地址表：配置组播地址表。交换机在转发组播数据时是根据组播地址表来进行的。 ● 组播过滤：配置组播过滤功能，可以限制用户对组播节目的点播。 ● 报文统计：查看各端口的组播报文流量，帮助您监控网络中IGMP报文。
第10章 路由功能	本模块用于配置交换机的组播路由功能，主要介绍了： ● 接口：配置三层接口。 ● 路由表：查看交换机的路由表。 ● 静态路由：为三层通信配置静态路由功能。 ● DHCP服务器：配置DHCP服务器功能，为以太网中的客户端分配IP参数。 ● DHCP中继：配置DHCP中继功能，使不同子网内的DHCP客户端可以共享DHCP服务器。 ● 代理ARP：配置代理ARP功能，为不同网络中的计算机提供ARP代理服务。 ● ARP：显示ARP表，可以查看本机中所有的静态或动态ARP条目。 ● RIP：配置交换机的RIP特性。 ● OSPF：配置交换机的OSPF特性。 ● VRRP：配置交换机的VRRP特性。
第11章 组播路由	本模块用于配置交换机的L3功能，主要介绍了： ● 全局配置：配置组播路由的全局参数和查看组播路由表。 ● IGMP配置：配置IGMP接口参数，静态组播组和组播过滤器等功能。 ● PIM DM：配置PIM DM接口和PIM DM邻居等相关参数。 ● PIM SM：配置PIM SM接口，候选BSR, BSR, 候选RP和静态RP等参数。 ● 静态组播配置：配置静态组播组的相关参数。
第12章 服务质量	本模块主要为网络中某些特殊应用程序提供保障，主要介绍了： ● QoS配置：给网络中的数据流划分优先级，保障重要数据的传输，可分为端口优先级、802.1P优先级和DSCP优先级。 ● 流量管理：可通过带宽控制来限制端口的数据流量；风暴抑制可限制局域网中各类广播包的传输带宽，节约网络资源。 ● 语音VLAN：在指定VLAN中传输语音数据，提高语音数据的传输优先级，保证通话质量。
第13章 访问控制	本模块通过配置对报文的匹配规则和处理操作来实现对数据包的过滤功能，有效防止非法用户对网络的访问，节约网络资源，主要介绍了： ● 时间段配置：通过时间段控制ACL条目的生效时间。 ● ACL配置：配置ACL条目。 ● Policy配置：配置ACL规则的处理方式。 ● 绑定配置：将Policy下发到端口和VLAN，使之正式生效。

章节	章节说明
第14章 网络安全	本模块针对局域网中常见的网络攻击进行防护，主要介绍了： ● 四元绑定：是将计算机的MAC地址和IP地址，所属VLAN以及连接交换机的端口号四者绑定。 ● IP源防护：对局域网中的IP数据包进行过滤。 ● DoS防护：对常见的DoS攻击进行防护。 ● 802.1X认证：配置交换机对局域网接入用户进行接入认证。
第15章 SNMP	SNMP提供了一个管理框架来监控和维护互联网设备。本模块主要用于配置交换机的SNMP功能，主要介绍了： ● SNMP配置：配置SNMP的基本属性。 ● 通知管理：配置SNMP通知管理，便于管理软件对交换机某些事件进行及时监控和处理。 ● RMON：配置RMON功能，便于网管更有效的监控网络。
第16章 LLDP	本模块用于配置LLDP功能，为SNMP提供部分信息，简化机器故障排除的过程，主要介绍了： ● 基本配置：配置LLDP的参数。 ● 设备信息：查看本地设备以及邻居设备的LLDP信息。 ● 设备统计：查看本地设备的LLDP相关统计信息。
第17章 集群管理	集群管理的主要目的是解决大量分散的网络设备的集中管理问题。模块主要用于配置交换机的集群管理功能，主要介绍了： ● 拓扑发现：配置拓扑发现功能。用于获取与其直接相连的邻居交换机的信息。 ● 拓扑收集：配置拓扑收集功能。用于命令交换机收集网络的拓扑信息。 ● 集群管理：配置集群管理功能。用于建立和维护集群。
第18章 系统维护	系统维护模块将管理交换机的常用系统工具组合在一起，主要介绍了： ● 运行状态：对交换机内存和CPU进行监控。 ● 系统日志：查看在交换机上配置的参数。 ● 系统诊断：检测与交换机连接的线缆及对端设备的可用性。 ● 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。
第19章 软件系统维护	主要介绍了：当交换机出现软件故障时，如何进入交换机的boot菜单重新加载软件。
附录A 802.1X客户端软件使用说明	主要介绍了如何使用我司提供的802.1X客户端软件，并利用该软件进行认证。
附录B 术语表	整理用户手册中出现的术语。
附录C 技术参数规格	技术参数规格表。

回目录

第2章 产品介绍

2.1 产品简介

T3700G-28TQ交换机是由普联技术有限公司为构建完整的大规模网络组网方案，自主研发设计的可堆叠三层网管交换机。

T3700G-28TQ具有4个万兆光纤模块扩展接口，支持RIP/OSPF/VRRP/PIM等丰富的三层路由功能，提供完备的安全策略、完善的QoS策略以及丰富的VLAN功能，易于管理维护，是理想的大型企业网、校园网的汇聚交换机以及中小企业、分支机构的核心交换机。

T3700G-28TQ的堆叠功能可支持多达8台设备互联形成一个堆叠系统进行统一管理，既可简化管理，又可增强网络的可靠性。T3700G-28TQ随机配送一个可拆卸的电源模块PSM150-AC，同时提供一个RPS输入接口用于连接外部冗余电源。可根据需要自行选购TP-LINK公司的冗余电源产品，与PSM150-AC互为备份为交换机供电，保障系统持续正常运行，增强网络稳定性。

2.2 产品特性

实用方便的路由功能

- 动态路由

支持RIP、OSPF两种主流的动态路由协议，能够解决各类中大型网络进行子网划分后的路由选路问题，简化网络配置。

- 静态路由

支持多条静态路由条目，通过简单的配置即可实现跨网段的通信,合理设置和使用静态路由,可有效改善网络性能。

- ARP代理

当计算机没有配置默认网关或者网络进行VLSM子网划分时，应用ARP代理功能，当网关收到源计算机向目标网络计算机发送的ARP请求时，使用自己的MAC地址与目标计算机的IP地址进行ARP应答，轻松实现不同网络间的互访。

- DHCP服务器

可作为DHCP服务器为DHCP客户端分配IP地址。能给不同VLAN指定特定的IP地址池，实现给不同的VLAN分配不同网段的IP地址。

- DHCP中继

支持DHCP中继功能，能为不同网段的DHCP客户端和DHCP服务器提供DHCP中继服务，将DHCP协议报文跨网段转发，使不同网段的DHCP客户端能共享一个DHCP服务器，有效降低网络组网成本。

完备的网络接入安全策略

- 一键快速绑定

支持PORT/MAC/IP/VLAN ID四元绑定，提供手动添加、自动扫描、DHCP侦听三种绑定方式，支持跨VLAN扫描，根据不同网络环境，轻松实现快速绑定。

- IP源防护

利用在交换机中绑定的四元信息对IP包进行检查，过滤不符合四元绑定表的IP报文，只处理与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

- DoS攻击防护

通过解析IP数据包，查看数据包中的特定字段是否符合DoS攻击数据包的特征，并采取相应的防护措施，直接丢弃非法数据包或者对合法的数据包进行限速。

- 防MAC地址攻击

支持端口安全特性，可以有效防御MAC地址攻击。可以实现基于MAC地址允许或限制流量，每个端口允许设定最大MAC地址数量，支持静态配置或交换机动态学习，全面保障网络安全。

多层次，多元化的访问控制策略

- 访问控制（ACL）

强大硬件ACL能力，深度识别报文，支持L2~L4数据流分类，提供基于源MAC、目的MAC、源IP地址、目的IP地址、IP协议类型、TCP/UDP端口等定义ACL。

- 策略控制（Policy）

支持基于端口、VLAN下发ACL，对符合相应ACL规则的数据包实现流分类，可进行流镜像、流监控和端重定向口三种行为控制，轻松实现网络监控，数据流量控制和数据转发控制。

- 时间段控制

新增基于时间段的ACL控制，提供节假日、绝对时间、周期以及时间片段设置功能，多种时间段的灵活组合可轻松实现对时间精确控制的访问需求。

- 802.1X认证

支持基于端口和基于MAC的802.1X认证，在用户接入网络时完成必要的身份认证，保证接入用户的合法性，支持Guest VLAN，轻松设置来宾用户接入访问权限。

丰富的VLAN特性

- IEEE 802.1Q VLAN

IEEE 802.1Q VLAN符合国际标准，完美融合了Port VLAN，与主流设备完全兼容，加上人性化的操作方式，使组网更加便捷、准确、高效。

- 协议VLAN

通过协议来划分VLAN，对特殊应用可设置自定义协议，实现安全通信。

- VLAN VPN（QinQ）

有效扩展VLAN资源，实现用户VLAN的透传技术，便于在智能小区、企业网或园区网中组建多层交换网络。

- Private VLAN

将多个Secondary VLAN和一个Primary VLAN组成VLAN对，下层用户通过Secondary VLAN相互隔离二层报文，上层设备只需识别Primary VLAN。有效解决了上层VLAN资源紧缺及传统VLAN中的广播问题。

- GVRP

基于GARP的工作机制，用来维护设备中的VLAN动态注册信息，使得局域网内的VLAN配置更快捷、方便。

完善多业务融合能力

- QoS

支持基于端口、IEEE802.1p以及DSCP三种优先级模式，支持Equ、SP（Strict Priority）、WRR（Weighted Round Robin）、SP+WRR四种队列调度算法，每个端口8个输出队列，可以将不同优先级的报文映射到不同输出队列，保障关键业务数据优先处理，满足不同业务对基础网络的需求。

- 流量控制

带宽控制支持端口双向限速，限速的控制粒度为64Kbps；风暴抑制支持对广播包、组播包、UL包限速，避免网络资源被恶意浪费，提高网络效率。

- 语音VLAN

内置语音设备OUI地址识别功能，通过Voice VLAN技术，对语音流进行有针对性的QoS配置，能够很好的解决语音设备数据流优先级的调整问题，保证通话质量。

- 组播管理

支持IGMPV1/V2/V3，通过IGMP Snooping技术，能很好地支持组播应用，如IPTV、视频会议等等；支持组播VLAN，有效避免带宽浪费，减轻上游设备的组播负担；静态组播地址表减少学习时间，提高组播转发效率；未知组播报文丢弃功能，节省带宽，提高系统处理效率。

高可靠性设计

- 生成树

支持传统的STP/RSTP/MSTP二层链路保护技术，极大提高链路的容错、冗余备份能力，保证网络的稳定运行。支持TC（Topology Change）报文保护，避免当设备受到恶意的TC报文攻击时，频繁的删除操作给设备带来很大负担。同时还支持环路保护、根桥保护、BPDU保护、BPDU过滤等功能。

- 链路汇聚

提供手工汇聚、LACP两种汇聚模式，能有效增加链路带宽，提高链路的可靠性，同时可以实现负载均衡、链路备份。

- 环路监测

通过环路监测数据包检测交换机连接的网络中是否存在环路，当检测出环路时，交换机可以发出报警或同时阻塞端口，以提醒用户或避免引起广播风暴。

灵活、安全的网络管理

- 堆叠管理

支持堆叠管理技术，能够把多台物理设备互相连接起来，使其虚拟为一台逻辑设备，并将多台设备看成一台单一设备进行管理和使用，大大简化大型网络的配置管理工作。

- 系统管理

支持CLI命令行（Console，Telnet，SSHV1/V2），Web网管（HTTP、SSL V2/V3/TLSV1），SNMP（V1/V2c/V3）等多种管理方式。

- 安全管理

通过身份过滤检测技术，能够很好的解决设备安全管理难题，支持两级用户管理，提供管理人员数限制功能，增强配置安全性。

- 网络监控

支持端口双向数据监控，结合网络分析软件可以实时监控网络运行状态，RMON功能可以实现统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

- 系统维护

支持CPU、内存实时监控，支持VCT电缆检查以及端口环回测试，方便定位网络故障点，同时支持Ping、Tracert命令操作，轻松分析出现故障的网络节点。

- 系统日志

提供免费的日志服务器软件，为用户提供对设备系统日志的数据库统计分析功能，有效监控设备运行和网络状况。

- 集群管理

支持NDP(邻居发现)、NTDP（邻居拓扑发现）和Web集群管理，轻松打造“零费用、免软件”的统一管理方式，支持信息产业部相关标准，兼容其它主流厂商的集群管理。

2.3 产品外观

2.3.1 前面板

T3700G-28TQ前面板如图 2-1所示。

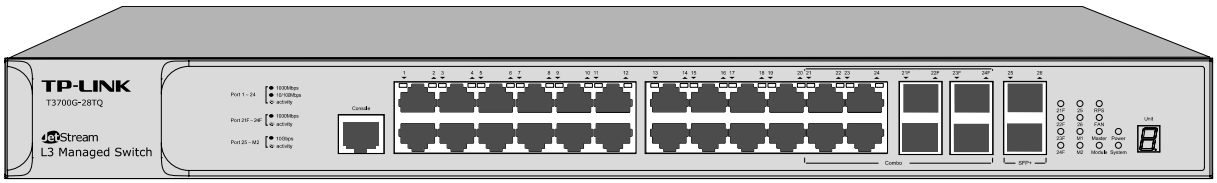


图 2-1 前面板

- **1个Console端口**

Console端口用于和计算机或其他终端的串口相连，可以通过命令行管理交换机。

- **24个10/100/1000Mbps自适应RJ45端口**

本系列交换机的1-24端口均支持10/100/1000Mbps带宽的连接设备的端口。每个端口对应一个Link/Act指示灯。

- **4个SFP端口**

端口21F~24F为SFP光纤模块扩展槽，用于安装SFP光纤模块。每个端口对应一个端口指示灯，分别标识为21F~24F。这4个端口分别与端口21~24共用，组成Combo口。Combo口中的两类端口只能使用一个，若同时连接了设备，则只有RJ45口工作，对应的SFP端口将失效。

SFP端口兼容多模、单模SFP光纤模块，只支持千兆光纤模块，推荐使用TP-LINK公司的千兆光纤模块，例如TL-SM311LM和TL-SM311LS。

- **2个SFP+端口**

端口25~26为10Gbps SFP+端口，用于安装SFP+光纤模块或SFP+铜缆。每个端口对应一个端口指示灯，分别标识为25、26。

T3700G-28TQ的后面板提供了一个接口模块扩展卡插槽，用户可根据需求自行选购TP-LINK公司的接口模块扩展卡（如TX432）进行安装，为交换机增加2个扩展的SFP+端口。

- **Unit ID数码指示灯**

用于显示交换机在堆叠系统中的成员编号。若交换机未加入任何堆叠系统，则显示系统的默认成员编号。可登陆交换机管理界面修改其默认成员编号，进入页面的方法为：**堆叠功能>>堆叠管理>>堆叠编号**。

- **指示灯**

通过指示灯您可以监控交换机的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态	描述
Power	电源指示灯	常亮	系统供电正常
		闪烁	系统供电异常
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮/熄灭	系统出现异常
		闪烁	系统正常工作
RPS	RPS指示灯	绿色常亮	热插拔电源模块及外部冗余电源均工作正常
		黄色常亮	热插拔电源模块出现故障，外部冗余电源工作正常
		不亮	未连接外部冗余电源
FAN	风扇指示灯	绿色常亮	内置风扇工作正常
		黄色常亮	内置风扇出现故障
Master	Master指示灯	常亮	1.交换机在堆叠系统中角色为Master 2.未加入任何堆叠系统
		不亮	交换机在堆叠系统中角色为Slave
Module	接口模块扩展卡指示灯	绿色常亮	接口模块扩展卡已安装且工作正常
		黄色闪烁	接口模块扩展卡出现故障
		不亮	未安装接口模块扩展卡
Link/Act (端口1-24)	端口指示灯	绿色常亮	端口与1000Mbps设备连接但没有数据传输
		绿色闪烁	端口与1000Mbps设备连接且正在接收或发送数据
		黄色常亮	端口与10/100Mbps设备连接但没有数据传输
		黄色闪烁	端口与10/100Mbps设备连接且正在接收或发送数据
		不亮	端口未连接网络设备
21F-24F	端口指示灯	常亮	端口已插入SFP光纤模块并连接1000Mbps设备，但没有数据传输
		闪烁	端口已插入SFP光纤模块并连接1000Mbps设备，且正在接受或发送数据
		不亮	端口未插入SFP光纤模块；或者已插入SFP光纤模块但未连接网络设备

指示灯	名称	状态	描述
25, 26	端口指示灯	常亮	端口已插入SFP+光纤模块或者SFP+铜缆，并连接10Gbps设备，但无数据传输
		闪烁	端口已插入SFP+光纤模块或者SFP+铜缆，并连接10Gbps设备，且正在接受或发送数据
		不亮	1.端口未插入SFP+光纤模块或SFP+铜缆 2.已插入SFP+光纤模块或SFP+铜缆但未连接设备
M1, M2	接口模块扩展卡端口指示灯	常亮	接口模块扩展卡端口已插入SFP+光模块或者SFP+铜缆，并连接10Gbps设备，但无数据传输
		闪烁	接口模块扩展卡端口已插入SFP+光纤模块或者SFP+铜缆，并连接10Gbps设备，且正在接受或发送数据
		不亮	1.未安装接口模块扩展卡 2.已安装接口模块扩展卡，但其对应端口未插入SFP+光纤模块或SFP+铜缆 3.对应端口已插入SFP+光纤模块或SFP+铜缆但未连接网络设备

2.3.2 后面板

交换机后面板如图 2-2所示：

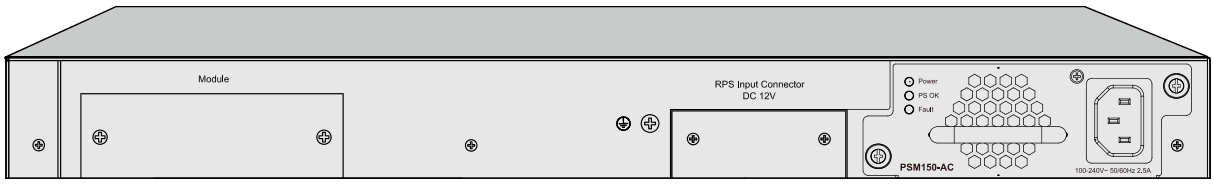


图 2-2 后面板一

为保护交换机，出厂时接口模块扩展卡插槽和RPS输入接口均安装了保护面板。移除所有保护面板，并将接口模块扩展卡TX432安装好后，交换机后面板如图 2-3所示：

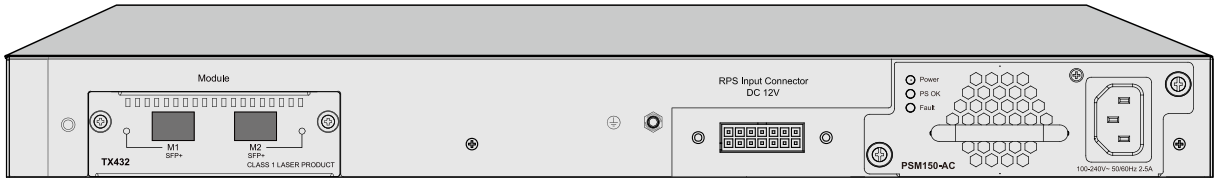


图 2-3 后面板二

- **接口模块扩展卡插槽**

用于扩展交换机的光纤模块接口。用户可根据需求自行选购TP-LINK公司的接口模块扩展卡（如TX432）进行安装，接口模块扩展卡的安装和拆卸方法请参考《安装手册》。

- **防雷接地柱**

请使用导线进行接地，以防雷击。为避免产品遭受雷击并延长产品的使用寿命，请参考光盘中的《防雷安装手册》进行防雷安装。

- **RPS输入接口**

用于连接冗余电源。用户可根据需求自行选购TP-LINK公司的冗余电源（如RPS150）进行连接，冗余电源的连接方法请参考《安装手册》。

- **电源模块**

交换机电源模块PSM150-AC为可拆卸电源，出现故障时可购买我司同型号电源替换，其接入电源需为100-240V~ 50/60Hz的交流电源。请务必使用原装电源线，并将电源插座安装安装在设备附近。

PSM150-AC支持热插拔，允许在交换机连接了冗余电源的情况下安装和拆卸本电源模块。电源模块的安装和拆卸方法请参考《安装手册》。

回目录

第3章 配置指南

3.1 登录Web页面

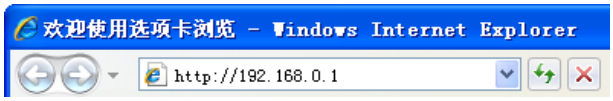
第一次登录时，请参考下面步骤登录交换机：

1) 交换机已正常加电启动，任一端口已与管理主机相连。

2) 在管理主机上安装IE 6.0或更高版本浏览器，同时显示器分辨率调整到1024×768或更高像素。

3) 设置管理主机IP地址交换机同一网段，即192.168.0.X/24（X为2至254之间的任意整数）。

4) 打开IE浏览器，在地址栏输入http://192.168.0.1登录交换机的Web页面。



5) 在登录界面中输入交换机管理帐号的用户名和密码，出厂默认值均为admin，如图 3-1所示。

图 3-1 登录页面

6) 成功登录后可以看到交换机的系统信息，如图 3-2所示。

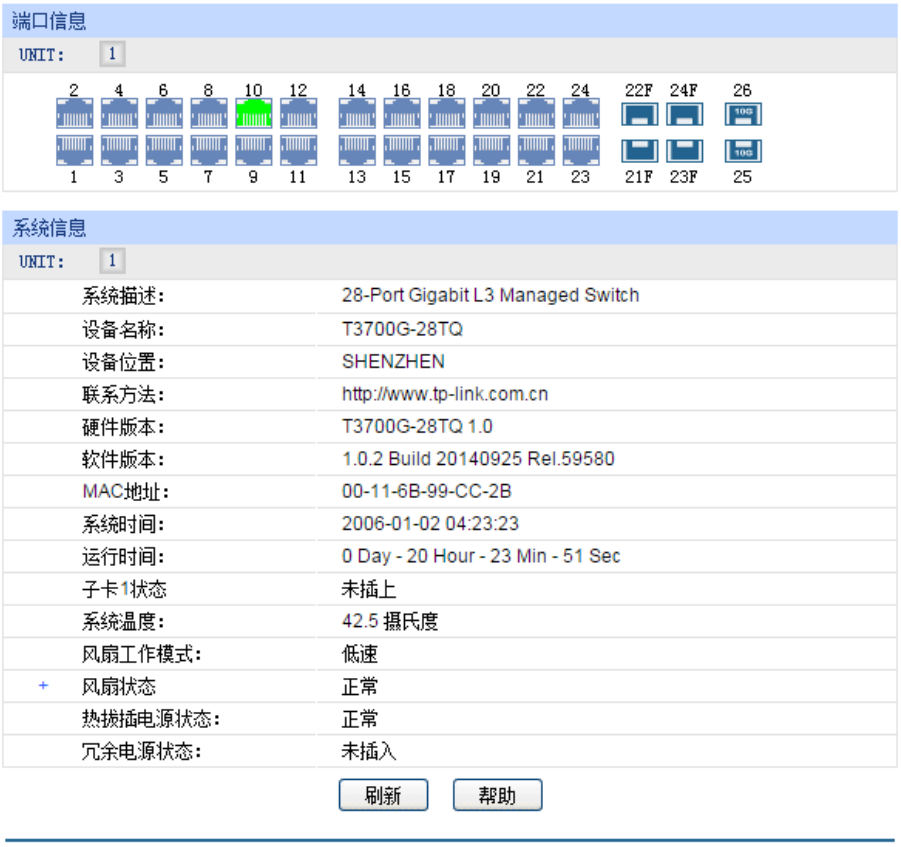


图 3-2 系统信息

3.2 Web页面简介

交换机典型的Web页面如图 3-3所示。

图 3-3 典型Web页面

在中可以看到，左侧为一级、二级功能菜单栏，右侧上方长条区域为各功能菜单下的标签页。标签页整体分为三部分，条目配置区、列表管理区以及提示注意区。

3.3 Web 配置注意事项

- **堆叠系统配置**

当网络中多台交换机建立堆叠后，连接登录任意一台堆叠成员的 Web 页界面将自动跳转到 Master 的 Web 界面。对于需要对全体堆叠成员生效的全局配置参数，提交保存后将自动推送配置参数到整个堆叠系统，使堆叠成员配置参数保持一致；对于接口相关的自定义参数，可以通过列表配置区上方的 UNIT 选择来配置对应成员的具体接口参数。

- **索引页面**

本交换机功能全面，基本覆盖了当前网络中用户的主流需求。通过一级菜单项**索引页面**，可以快速查询并定位至相应的功能页面。

- **配置保存**

配置交换机后，点击<提交>按键当前配置立即生效，但断电重启后配置参数将失效；若需要当前配置在交换机重启后依旧生效，则需要点击功能菜单栏底部的<配置保存>按钮保存配置参数。建议每次配置完成后均进行配置保存动作，或者在交换机断电或重启前完成该动作。

- **端口号介绍**

我司交换机的端口号格式为X/Y/Z。其中，X表示该端口所属的交换机在堆叠成员中的Unit ID；Y表示交换机上的扩展模块编号，主端口编号为0；Z表示交换机的端口号。

回目录

第4章 系统管理

系统管理模块主要用于配置交换机的系统属性，包括**系统配置**、**用户管理**、**系统工具**以及**安全管理**四个部分。

4.1 系统配置

系统配置用于配置交换机的基本属性，本功能包括**系统信息**、**设备描述**、**系统时间**和**夏令时**四个配置页面。

4.1.1 系统信息

本页面用来查看本交换机的端口连接信息和系统信息。

进入页面的方法：系统管理>>系统配置>>系统信息

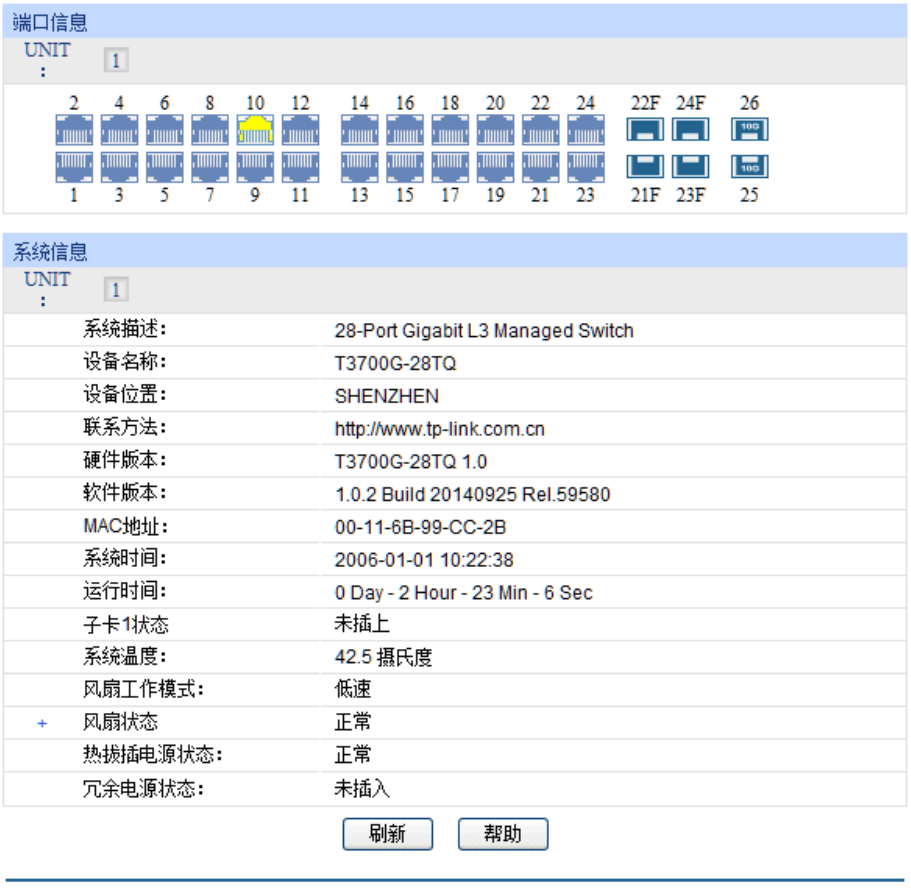


图 4-1 系统信息

条目介绍：

- **端口状态**


1000Mbps端口未接入设备。


1000Mbps端口工作速率为1000Mbps。


1000Mbps端口工作速率为100Mbps/10Mbps。


SFP端口未接入设备。

 　　SFP端口工作速率为1000Mbps。

 　　SFP+端口未接入设备。

 　　SFP+端口工作速率为10Gbps。

当鼠标移到某端口上时，会显示该端口的详细信息，如下图所示。

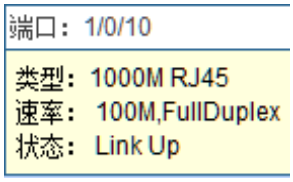


图 4-2 端口信息

条目介绍：

- **端口信息**

端口：	显示交换机的端口号。
类型：	显示端口的端口类型。
速率	显示端口当前的连接速率和传输模式。
状态：	现在端口的状态。

点击某端口，会显示此端口的带宽利用率，即实际传输速率与其最大传输速率的百分比，图中每隔4秒反馈一次监控值。查看各个端口的带宽利用率，可以帮助您及时了解各端口的流量概况，便于监控网络流量和分析网络异常。如下图所示。

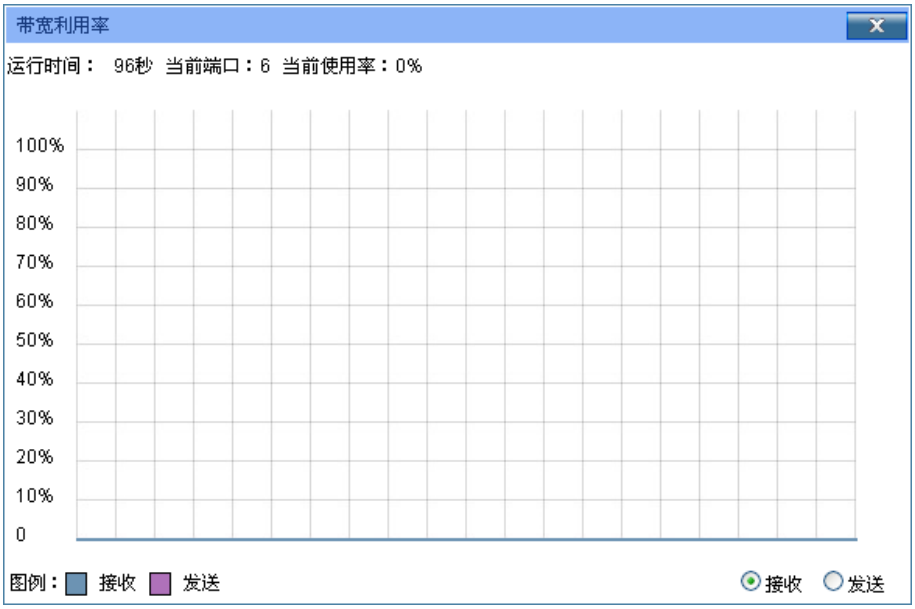


图 4-3 带宽利用率

条目介绍：

- **带宽利用率**

接收	点击后，显示此端口接收数据的带宽利用率。
发送	点击后，显示此端口发送数据的带宽利用率。

4.1.2 设备描述

本页面用来配置交换机的描述信息，包括设备名称、设备位置、联系方法。

进入页面的方法：系统管理>>系统配置>>设备描述

图 4-4 系统描述

条目介绍：

- **设备描述**

设备名称： 填写交换机的名称。

设备位置： 填写交换机的位置信息。

联系方法： 填写您的联系方法。

4.1.3 系统时间

本页面用来配置交换机的系统时间。系统时间是交换机工作时使用的时间，其它功能（如访问控制）中的时间信息以此处为准。可以选择手动设置时间或者连接到一个NTP（网络时间协议）服务器获取UTC时间，也可以获取当前管理PC的时间作为交换机的系统时间。

进入页面的方法：系统管理>>系统配置>>系统时间

图 4-5 系统时间

条目介绍：

- **时间信息**

当前系统时间： 显示交换机当前的日期、时间。

当前时间来源： 显示交换机当前系统时间的来源。

➢ **时间配置**

手动配置时间： 勾选后，手动配置日期、时间。

从NTP服务器获取时间： 勾选后，配置时区和NTP服务器的IP地址，交换机将自动获取UTC时间。此时交换机必须连接至NTP服务器。

- 时区：选择您所在的时区。
- 首选/备选NTP服务器：填写NTP服务器的IP地址。
- 更新周期：设定从NTP服务器获取时间的周期。

从管理PC获取时间： 勾选后，将管理主机的时间配置为交换机的系统时间。

注意：

- 如果向指定的时间服务器请求时间不成功，交换机会选择向上一次成功获取时间的服务器地址和网络上默认的公用时间服务器地址来获取时间。

4.1.4 夏令时

本页面用来配置交换机的夏令时。

进入页面的方法：系统管理>>系统配置>>夏令时

图 4-6 夏令时

条目介绍：

➢ **夏令时配置**

夏令时状态： 选择是否启用夏令时功能。

预定义模式： 选择一个预先定义好的夏令时配置。

- 美国：三月第二个星期天02:00 ~ 十一月第一个星期天02:00。
- 澳大利亚：十月第一个星期天02:00 ~ 四月第一个星期天03:00。
- 欧洲：三月最后一个星期天01:00 ~ 十月最后一个星期天01:00。
- 新西兰：九月最后一个星期天02:00 ~ 四月第一个星期天03:00。

循环模式： 配置夏令时功能。在这一模式下做的配置可以循环使用。

- 偏移：指定当夏令时来临时，需要调整的时间额度。单位为分钟。
- 开始/结束时间：分别选择夏令时开始和结束的时间。

日期模式：	配置夏令时功能。在这一模式下做的配置只能生效一次（开始时间的年份为当前年份）。 ● 偏移：指定当夏令时来临时，需要调整的时间额度。单位为分钟。 ● 开始/结束时间：分别选择夏令时开始和结束的时间。

4.2 用户管理

用户管理用来限制登录交换机Web页面的用户的访问权限和身份，以保护交换机的有效配置。

本功能包括**用户列表**和**用户配置**两个配置页面。

4.2.1 用户列表

可以在本页查看到当前交换机存在的全部用户。

进入页面的方法：系统管理>>用户管理>>用户列表

图 4-7 用户列表

4.2.2 用户配置

本页用来配置登录交换机Web页面的用户的身份类型。本交换机提供两种类型的用户：受限用户和管理员。受限用户，仅可以查看部分功能的配置数据，不能对交换机进行任何配置；管理员，可以配置交换机的全部功能。本说明书内如无特殊说明，均以“管理员”身份登录时的Web页面为准。

进入页面的方法：系统管理>>用户管理>>用户配置

图 4-8 用户配置

条目介绍：

➢ **用户信息**

用户名：	填写登录Web页面的用户名。

用户类型： 选择该用户名的用户类型。

- 管理员：可以编辑、修改和查看交换机各个功能的配置。
- 受限用户：仅可以查看交换机各个功能的配置情况。

密码： 填写该用户名的登录密码。

确认密码： 再次输入该用户名的登录密码，两次输入的密码需保持一致。

密码显示模式： 当导出配置文件时，登录密码将以此处设置的方式显示。

- 简单：在配置文件中，用明文显示密码。
- 加密：在配置文件中，用密文显示密码。

➢ **用户列表**

选择： 勾选条目进行删除，可多选。但是不可以对当前登录用户自身进行删除。

序号、用户名、类型： 显示当前用户的序号、用户名和用户类型。

操作： 点击对应条目的<编辑>按键，可以修改该条目的用户信息。修改完毕后点击<修改>按键，修改内容生效。但是不允许修改当前登录用户自身的用户类型和状态。

4.3 系统工具

系统工具功能集中对交换机的配置文件进行管理，包括**启动参数**、**配置导入**、**配置导出**、**软件升级**、**系统重启**和**软件复位**六个配置页面。

4.3.1 启动参数

本交换机可以预先上传两个启动镜像文件，在本页面中可以查看和修改交换机的启动参数，交换机上电后用启动镜像启动，如果失败则尝试使用备份镜像启动。交换机启动后会尝试读取启动配置，如果失败则读取备份配置。如果备份配置也读取失败，则交换机将自动恢复为出厂配置。

进入页面的方法：系统管理>>系统工具>>启动参数

图 4-9 启动参数

条目介绍：

➢ **启动参数**

选择： 勾选条目编辑交换机的启动参数。

成员： 显示选中条目的Unit ID。

当前镜像： 显示当前启动所用到的镜像名称。

启动镜像： 选择下一次启动的主镜像。

备份镜像： 选择备份镜像。如果无法从启动镜像启动，则使用备份镜像启动。

当前配置： 显示当前启动所用到的配置文件。

启动配置： 输入用于下一次启动的主配置文件名。

备份配置： 输入备份配置文件名。

重置： 点击<重置>按钮使交换机的启动参数恢复出厂默认值。

- **镜像列表**

显示交换机的镜像列表以及状态。

4.3.2 配置导入

配置导入功能是将以前备份的配置文件导入至交换机中，使交换机恢复到当时的配置状态。

进入页面的方法：系统管理>>系统工具>>配置导入

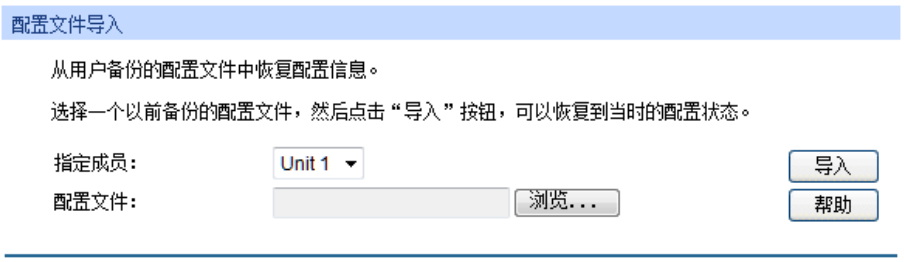


图 4-10 配置导入

条目介绍：

- **配置文件导入**

指定成员： 根据Unit ID选择交换机导入配置文件。

导入配置文件： 将备份文件中保存的配置信息恢复到当前状态，交换机自动重启后配置生效。

注意：

- 恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。
- 导入配置文件的过程不能关闭交换机电源，否则将导致交换机损坏而无法使用。
- 导入配置文件后，交换机中原有的配置信息将会丢失。如果您导入的配置文件有误，可能会导致交换机无法被管理。

4.3.3 配置导出

配置导出功能是将交换机当前的配置信息打包成文件保存到PC中，方便您日后通过该文件恢复配置。

进入页面的方法：系统管理>>系统工具>>配置导出

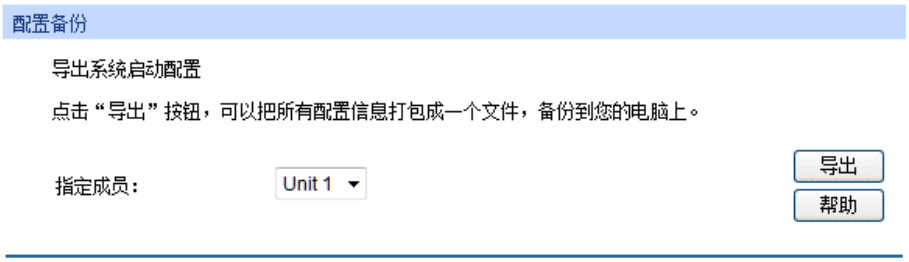


图 4-11 配置导出

条目介绍：

- **配置文件备份**

指定成员： 根据Unit ID选择交换机导出其配置文件。

备份配置文件： 以文件形式保存您的设置。建议升级前导出配置文件进行备份。

注意：

- 备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

4.3.4 软件升级

本交换机可以通过Web方式升级系统文件，系统升级后将获得更完善的功能，请在http://www.tp-link.com.cn网站上下载最新版本的系统文件。

进入页面的方法：系统管理>>系统工具>>软件升级

图 4-12 软件升级

注意：

- 升级过程中不能被中断。
- 升级时请选择与当前硬件版本一致的软件。
- 升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。
- 升级完成后，设备会自动重启。
- 建议升级前备份您的配置信息。

4.3.5 系统重启

在此处可以重新启动交换机，交换机重启后自动返回到登录页面。重启前请先保存当前配置，否则重启后，未保存的配置信息将丢失。

进入页面的方法：系统管理>>系统工具>>系统重启

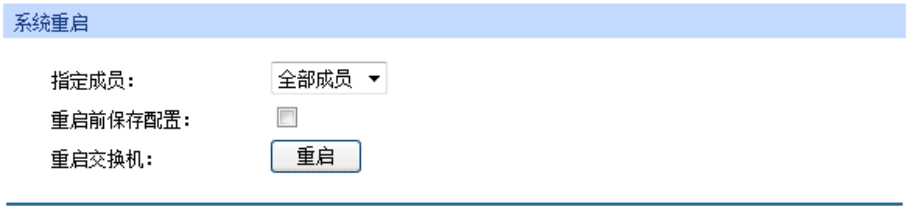


图 4-13 系统重启

注意：

- 在设备重启期间，请不要关闭设备电源，以免损坏设备。

4.3.6 软件复位

通过软件复位，可以将交换机恢复为出厂设置状态，所有配置数据将被清除。

进入页面的方法：系统管理>>系统工具>>软件复位

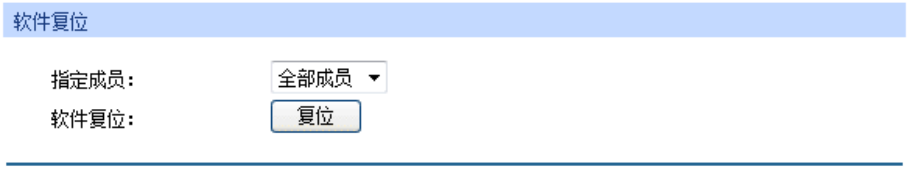


图 4-14 软件复位

4.4 安全管理

安全管理功能是针对不同的远程登录方式，采取相应的安全措施，以增强用户管理交换机的安全性。包括**安全配置**、**SSL配置**、**SSH配置**三个配置页面。

4.4.1 安全配置

本页用来限制登录交换机Web页面的用户的身份及人数，从而增强了交换机配置管理的安全性。其中，管理员及受限用户的定义请参考4.2用户管理。

进入页面的方法：系统管理>>安全管理>>安全配置

图 4-15 安全配置

条目介绍：

- **身份限制**

限制类型： 选择限制用户身份的类型。

- 基于IP：限制访问交换机Web页面的管理主机的IP网段。
- 基于MAC：限制访问交换机Web页面的管理主机的MAC地址。
- 基于端口：限制访问交换机Web页面的交换机端口号。

IP地址、掩码： 选择“基于IP”时才能进行配置。只允许指定IP网段的用户才可以通过Web页面管理交换机。

MAC地址： 选择“基于MAC”时才能进行配置。只允许指定MAC地址的用户才可以通过Web页面管理交换机。

端口号： 选择“基于端口”时才能进行配置。只允许通过指定交换机端口管理交换机。

- **超时配置**

超时时间： 如果在超时时间之内没有对交换机管理页面进行操作，系统会自动退出管理页面，若要再次进行管理请重新登录。默认为10分钟。

- **管理人数限制**

人数限制功能： 选择是否启用人数限制功能。

管理员人数： 填写可同时登录交换机Web页面的管理员总数。

受限用户人数： 填写可同时登录交换机Web页面的受限用户总数。

4.4.2 SSL配置

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于TCP的应用层协议提供安全连接，如为普通的HTTP连接提供更安全的HTTPS连接。SSL协议广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输，多使用在电子商务、网上银行等领域，为网络上数据通讯提供安全性保证。

SSL协议提供的服务主要有：

1. 对用户和服务器进行基于证书的身份认证，确保数据发送到正确的用户和服务器；
2. 对传输数据进行加密，以防止数据中途被窃取；
3. 维护数据的完整性，确保数据在传输过程中不被改变。

SSL采用非对称加密技术，使用“密钥对”进行数据的加密/解密，“密钥对”由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名）和对应私钥，也可以通过证书/密钥导入功能替换默认的密钥对，但SSL证书/密钥必须配对导入，否则HTTPS不能正常连接。

本功能生效后，即可通过https://192.168.0.1登录交换机的Web页面。初次使用交换机默认的证书通过HTTPS登陆交换机时，浏览器可能会提示“该证书是自签名的而不被信任”或“证书错误”，此时请将此证书添加为信任证书，或者继续浏览此网站即可。

进入页面的方法：系统管理>>安全管理>>SSL配置

图 4-16 SSL证书管理

条目介绍：

- **SSL证书管理**

  SSL功能： 选择是否启用交换机的SSL功能。

- **证书导入**

  SSL证书： 选择要导入的SSL证书。证书必须为BASE64编码格式。

- **密钥导入**

  SSL密钥： 选择要导入的SSL密钥。密钥必须为BASE64编码格式。

注意：

- SSL证书/密钥必须配对导入，否则HTTPS不能正常连接。
- SSL证书/密钥导入后，需要重启交换机才能生效。
- 要使用HTTPS建立安全连接，必须在浏览器的地址栏指定“https://提示符”。
- HTTPS连接涉及身份认证、加密、解密等过程，故响应速度可能会比普通的HTTP连接稍慢。

4.4.3 SSH配置

SSH（Secure Shell，安全外壳）是由IETF（Internet Engineering Task Force，因特网工程任务组）所制定，建立在应用层和传输层基础上的安全协议。SSH加密连接所提供的功能类似于一个telnet连接，但是传统的telnet远程管理方式在本质上是不安全的，因为它在网络上是使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

SSH是由服务器端和客户端组成的，并且有V1和V2两个不兼容的版本。在通讯过程中，SSH服务器与客户端会自动互相协商SSH版本号和加密算法，协商一致后，由客户端向服务器端发起请求登录的认证请求，认证通过后双方即可进行信息的交互。本交换机支持SSH服务器功能，可以使用SSH客户端软件通过SSH连接方式登录交换机。

SSH密钥导入是将SSH的公钥文件导入至交换机中。如果密钥导入成功，交换机会优先选用密钥认证的方式接受SSH登入。

进入页面的方法：系统管理>>安全管理>>SSH配置

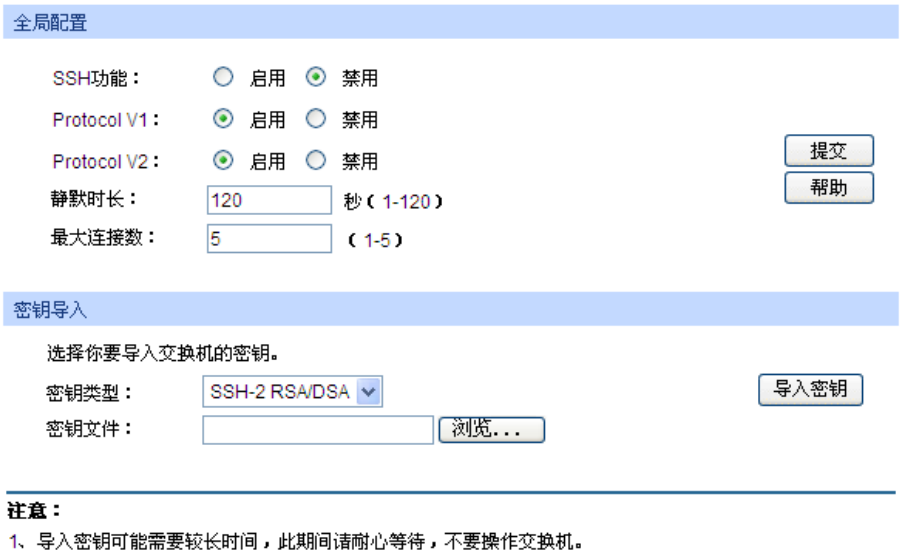


图 4-17 SSH配置

条目介绍：

- **全局配置**

SSH功能： 选择是否启用SSH功能。

Protocol V1： 选择是否启用对SSH V1的支持。

Protocol V2： 选择是否启用对SSH V2的支持。

静默时长： 填写静默时长。该时间内客户端无任何操作时，连接会自动断开。默认为120秒。

最大连接数： 填写SSH同时可允许的最大连接数，连接数若满，将无法再建立新的连接。默认为5。

➢ **密钥导入**

密钥类型： 选择所要导入的密钥类型。本机支持SSH-1 RSA,SSH-2 RSA和SSH-2 DSA三种类型的密钥。

密钥文件： 选择要导入的密钥文件。

导入密钥： 点击此按键，将所选的SSH密钥导入交换机。

注意：

- 请确保导入的文件是密钥长度为256至3072比特的SSH公钥。
- 导入密钥文件后，交换机中此用户原有的同类型密钥将会被覆盖。如果您导入的密钥文件有误，SSH会转用密码认证的方式登陆。

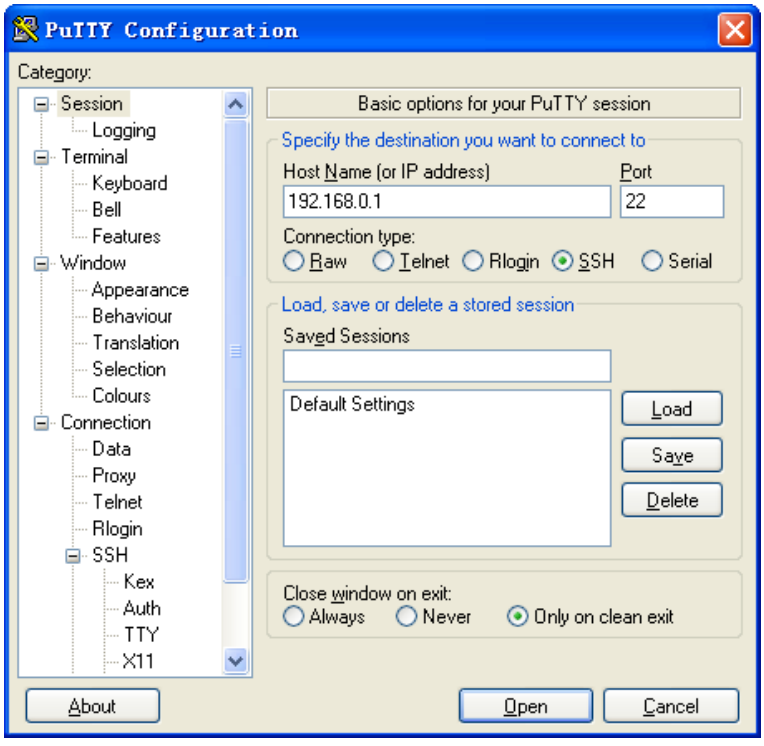
4.4.4 组网应用一

➢ **组网需求**

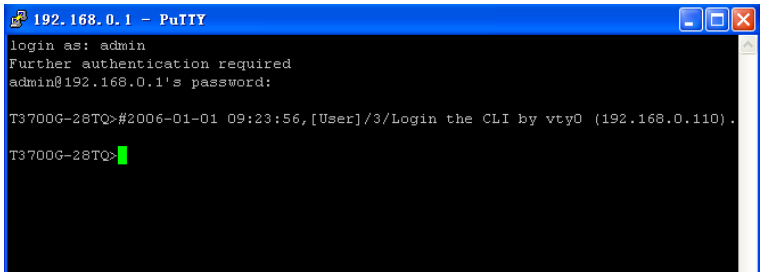
1. 使用 SSH 功能的“密码认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➢ **配置步骤**

1. 打开软件，登录 PuTTY 的主界面。在“Host Name”处填写交换机的 IP 地址；“Port”保持默认的 **22**；“Connection type”处选择 **SSH** 的接入方式。如下图所示。



2. 点击<Open>按键，即可登录到交换机。操作方法与 telnet 相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。



注意：

- 完成上述配置步骤后，Putty 客户端显示“T3700G-28TQ>”表明您已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在超级终端上设置该密码。详细步骤请参考《命令行手册》中的 **1.1.2 配置特权模式密码**。

4.4.5 组网应用二

➢ **组网需求**

1. 使用 SSH 功能的“密钥认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➢ **配置步骤**

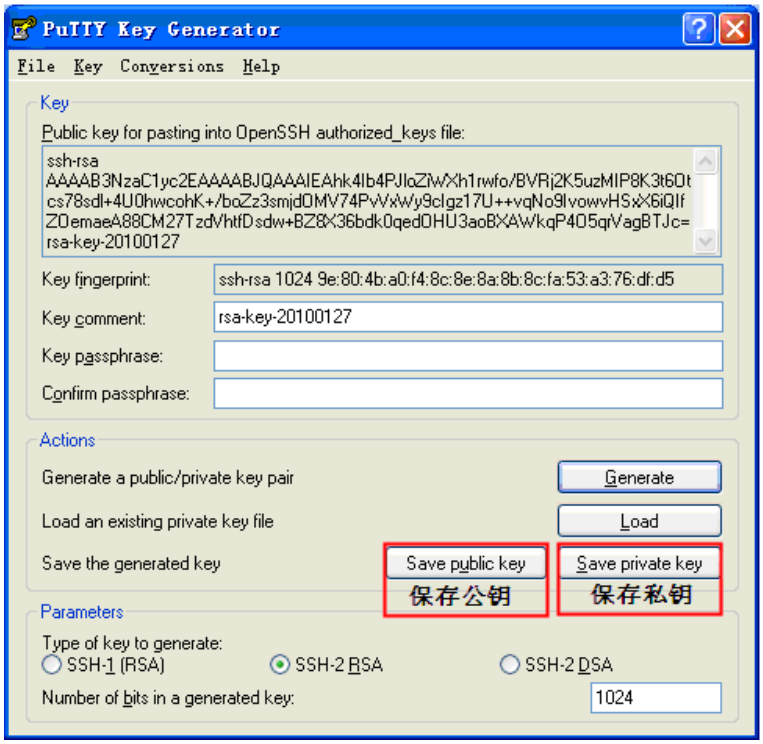
1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。

注意：

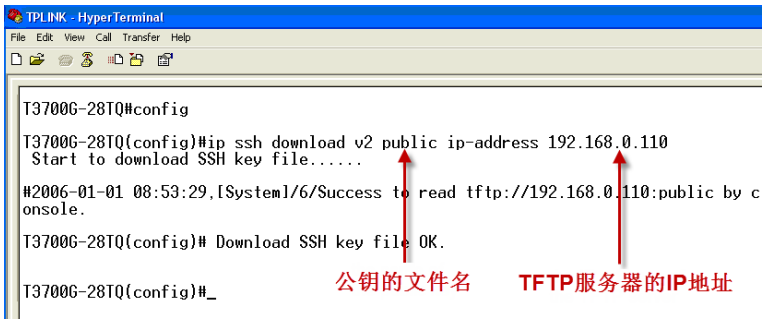
- 密钥长度的范围为 256 至 3072 比特。

- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

2. 密钥生成后，将公钥和私钥文件保存在主机上。如下图所示。



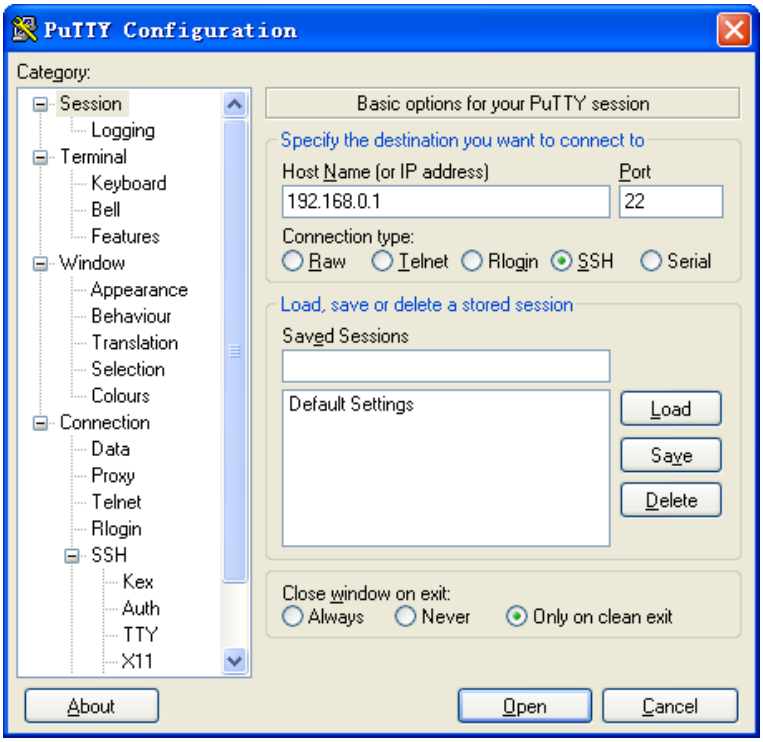
3. 在超级终端上，将保存至 TFTP 服务器上的公钥文件导入交换机中。



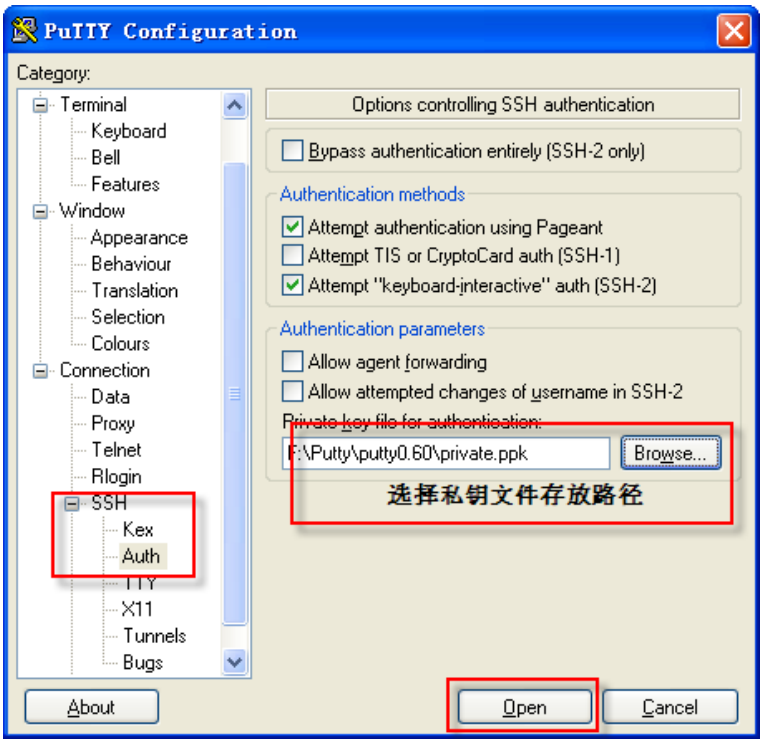
注意:

- 密钥类型要与密钥文件的类型保持一致。
- 载入 SSH 密钥的过程不能被中断。

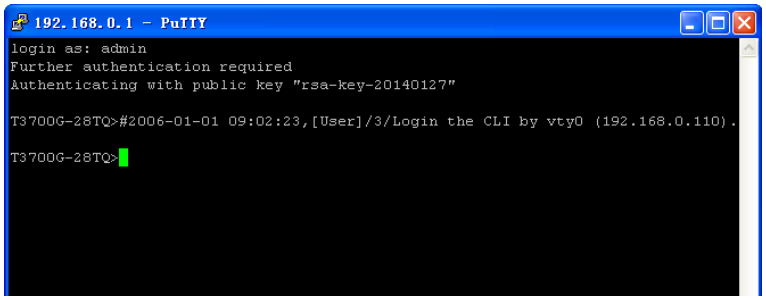
4. 打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH，如下图所示。



5. 点击左边的目录栏进入 SSH 目录下的 Auth 菜单，将私钥文件导入至 SSH 客户端软件中，再点击<open>按钮与服务器建立连接并进行协商。如下图所示。



6. 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。



注意:

- 完成上述配置步骤后，Putty 客户端显示“T3700G-28TQ>”表明您已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在超级终端上设置该密码。详细步骤请参考《命令行手册》中的 **1.1.2 配置特权模式密码**。

回目录

第5章 堆叠管理

堆叠（Stack）是指将多台设备通过专用的堆叠口连接起来，进行必要的配置后，虚拟化成一台“分布式设备”。使用堆叠技术可以实现多台设备的协同工作和统一管理，对外表现就像一台设备一样。

- **堆叠的优点**

堆叠主要具有以下优点：

1. 简化管理。堆叠系统形成后，用户可以通过任意成员设备的任意端口登录堆叠系统，将整个堆叠系统看成一台设备进行统一管理，多台设备只需配置一次。用户可以通过 CONSOLE、SNMP、TELNET、WEB 等多种方式来管理整个系统。
2. 高可靠性。堆叠系统的高可靠性体现在多个方面，例如：

   1）冗余备份：堆叠系统由多台成员设备组成，Master 设备负责堆叠系统的运行、管理和维护，其他成员设备在处理业务的同时可作为 Master 的备份。一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证业务不中断，从而实现了设备的 1：N 备份。由于在堆叠系统运行过程中实行了严格的配置同步和数据同步，新 Master 能接替原 Master 继续管理和运营堆叠系统，而不会影响系统的正常工作。

   2）分布式链路聚合：支持跨设备的链路聚合。由于堆叠系统对外可看做一台设备，外部设备可同时连接在不同的堆叠成员设备上并形成链路聚合，这些链路之间可以进行负载分担和互为备份，从而提高堆叠系统的可靠性，同时还可以极大的简化网络拓扑，如图 5-1 所示。

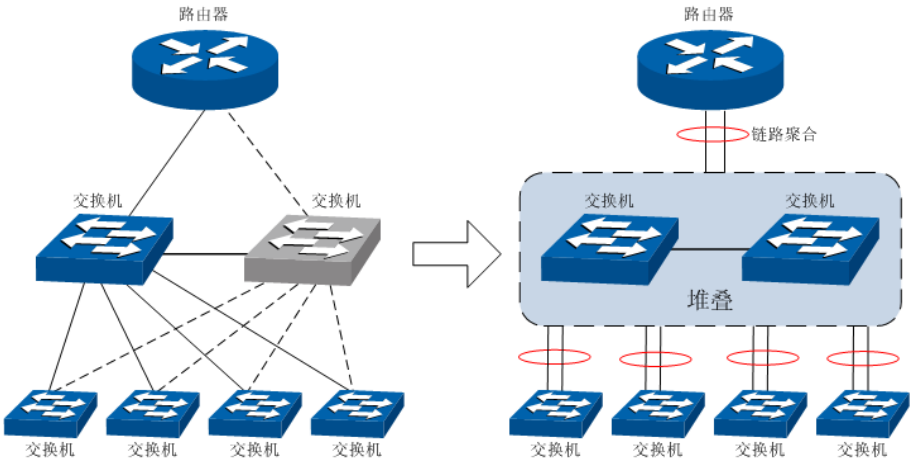


图 5-1 跨设备的链路聚合

对于拓扑为环形连接的堆叠系统，当有设备或链路故障时，会变成链形连接的堆叠继续正常工作，因此堆叠系统内的成员设备及链路之间也可进行负载分担和互为备份，如图 5-2 所示。

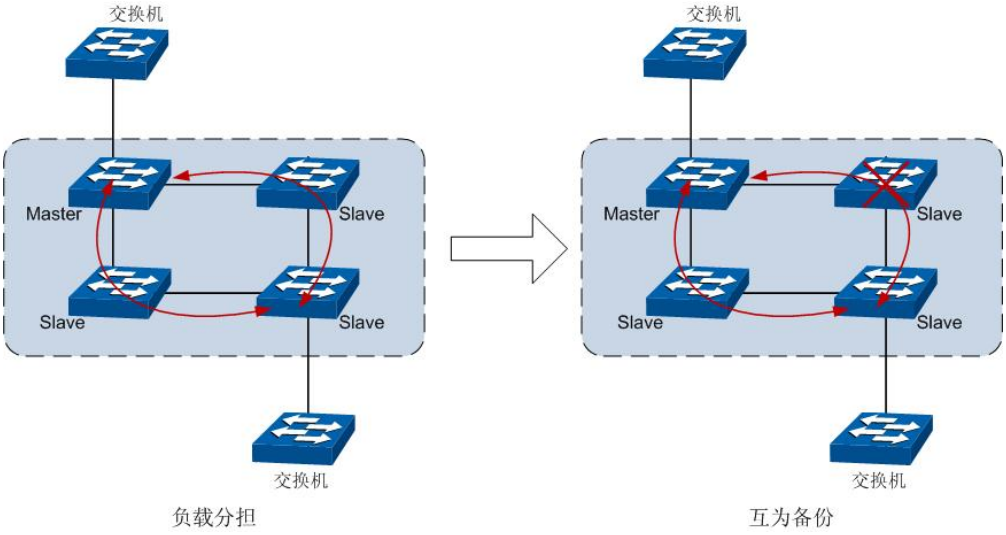


图 5-2 成员设备间的负载分担和互为备份

3. 强大的网络扩展能力。由于堆叠系统中的每个成员设备都能够独立处理协议报文、进行数据转发，所以增加成员设备即可扩展堆叠系统的端口数、带宽。用户可根据需要任意增减堆叠成员数，而不会影响堆叠系统的正常工作，在网络升级时可以最大限度的保护已有投资。

- **典型组网应用示例图**

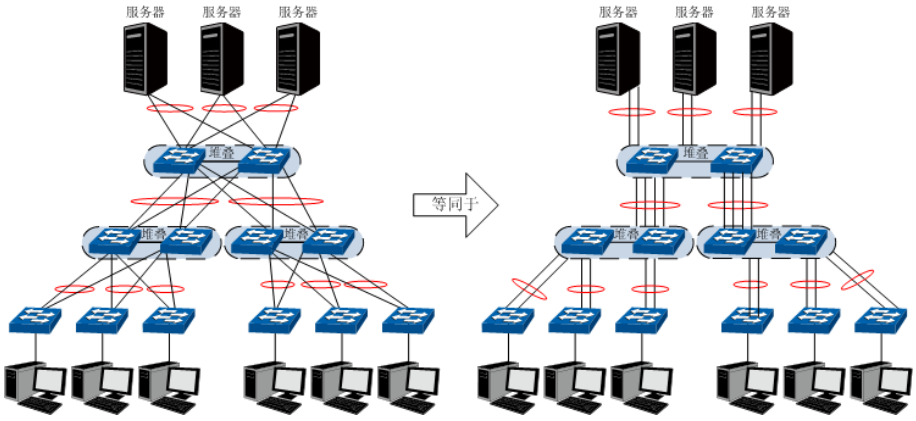


图 5-3 典型组网示意图

- **堆叠的原理**

1. 基本概念

1）角色

堆叠系统中每台设备都称为成员设备。各成员设备在正常处理业务报文的同时，按照在堆叠系统中功能的不同，分为两种角色：

- **Master**：负责管理整个堆叠系统。
- **Slave**：Master 设备的备份。当 Master 故障时，系统会自动从 Slave 中选举一个新的 Master 接替原 Master 的工作。

2） 系统事件

系统事件指的是在堆叠系统中可能发生的几种全局事件，主要有以下两种：

- **合并（merge）**：两个已经各自稳定运行的堆叠系统，通过物理连接和必要的配置后，形成一个新的堆叠系统。如下图所示：

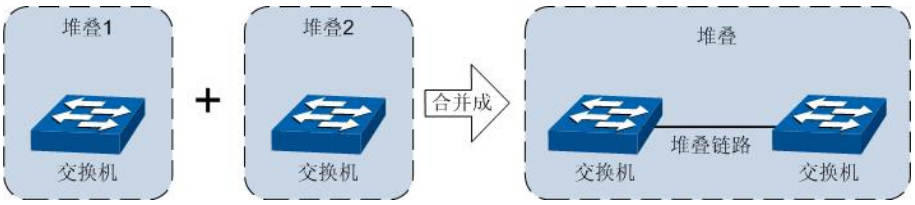


图 5-4 堆叠合并

堆叠系统合并时，原 Master 之间会进行竞争，得到一个新的 Master。竞争失败方的所有成员设备均以 Slave 的角色加入获胜方，最终合并为一个堆叠系统。Master 会为这些新加入的成员分配成员编号，并对其配置文件进行比较，所有全局配置与当前 Master 不同的成员设备均重新配置，统一采用 Master 的配置。

- **分裂(split)**：一个堆叠系统因为内部链路中断，导致分裂成两个或多个堆叠系统。如下图所示：

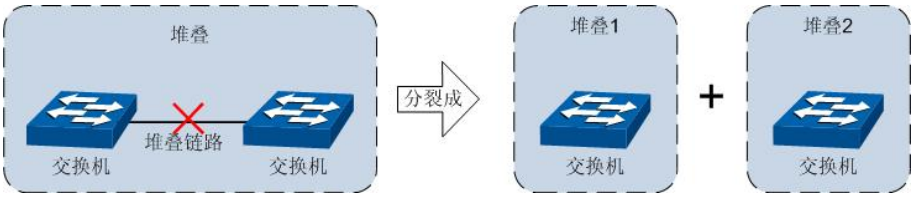


图 5-5 堆叠分裂

堆叠系统分裂后，每一个新的堆叠系统都会选举出自己的新 Master，并使用新 Master 的 MAC 地址作为新堆叠系统的 MAC 地址。由于各个新堆叠系统都会继续使用原堆叠系统的 IP 地址，所以堆叠分裂可能导致网络中产生三层协议的冲突。

2. 工作原理

堆叠系统将经历物理连接、拓扑收集、角色选举、堆叠管理与维护四个阶段。

1） 物理连接

用网线将交换机的堆叠口连接起来即可。T3700G-28TQ 系列交换机的堆叠口既可以用于堆叠连接，也可以用作普通万兆口。因此，在建立堆叠系统时，需将堆叠口的堆叠口模式设置为 Stack。如果堆叠口模式为 Ethernet，则此堆叠口将作为普通以太网口工作。

堆叠系统的连接拓扑有两种：链形连接和环形连接，如图 5-6 所示。

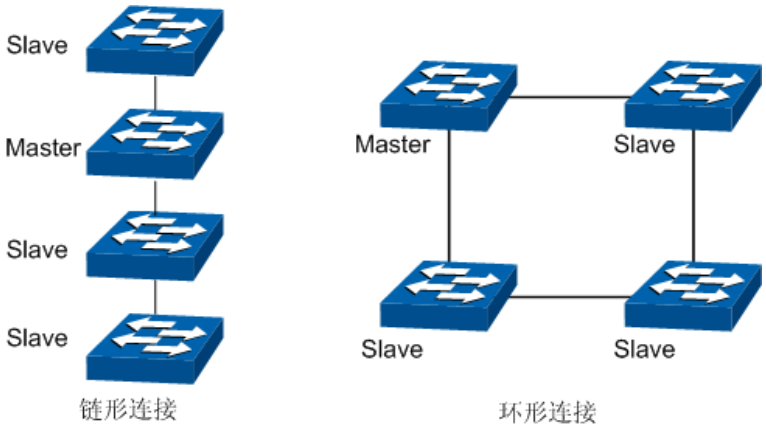


图 5-6 堆叠连接拓扑

- 链形连接对成员设备的物理位置要求较低，主要用于成员设备物理位置分散的组网。
- 环形连接比链形连接更可靠。因为当链形连接中出现链路故障时，会引起堆叠分裂；而环形连接中某条链路故障时，会形成链形连接，堆叠系统的业务不会受到影响。

注意：

用户最多可以使用 8 台 T3700G-28TQ 系列交换机建立链形或环形堆叠。

3）拓扑收集

堆叠系统中各成员设备通过与邻居设备交换堆叠 Discovery 报文来收集整个堆叠系统的拓扑。Discovery 报文会携带拓扑信息，具体包括堆叠端口连接关系、成员设备编号、成员设备优先级、成员设备的 MAC 地址等内容。

每个成员设备在本地记录自己已知的拓扑信息。设备刚启动时只记录了自身的拓扑信息。各成员设备会将已知的拓扑信息周期性的从堆叠端口发送出去；直接邻居收到该信息后，会更新本地记录的拓扑信息；如此往复，经过一段时间的收集，所有成员设备都会收集到完整的拓扑信息（称为拓扑收敛）。

此时会进入角色选举阶段。

4）选举 Master

拓扑收集完成后，系统开始角色选举。一个堆叠系统中只有一个 Master，其余设备为 Slave。确定哪个成员设备为 Master 的过程称为角色选举。

角色选举会在堆叠拓扑变更的情况下产生，比如堆叠建立、堆叠合并、堆叠分裂、堆叠系统或者当前 Master 重启等。

选举 Master 的规则为：

（1）当前是 Master 的优先；

（2）成员优先级大的优先；

（3）如果成员优先级相同，则 MAC 地址小的优先。

角色选举完成后，堆叠系统形成，进入堆叠管理与维护阶段。

注意：

1. 成员优先级的取值范围为 1-15，值越大，优先级越高，当选为 Master 的可能性越大。设备的缺省成员优先级均为 1，如果想让某台设备当选为 Master，可在组建堆叠前，通过手动配置提高该设备的成员优先级。
2. 设备在冷启动加入堆叠系统时是非抢占模式的，具体过程如下：设备刚启动时默认为无角色状态，它通过发送 Discovery 报文搜集当前堆叠的拓扑，当拓扑搜集完成之后，设备将按照上述的选举规则来确定自己的角色。如果检测到有 Master 存在，则该设备自动成为 Slave，即使它拥有更高的优先级，也不会抢占当前 Master 的地位。

5）堆叠管理与维护

堆叠系统形成后，所有的成员设备组成一台虚拟设备存在于网络中，由 Master 统一管理。下面简要介绍堆叠管理过程中的相关概念及规则。

- **成员编号：**堆叠系统运行过程中，使用成员编号（Unit ID）来标志和管理成员设备。在一个堆叠系统中，成员编号是唯一的。交换机出厂时默认的成员编号都为 1，为保证成员编号的唯一性，建议在建立堆叠前，统一规划各成员设备的编号，并逐一进行手工配置。

  在堆叠建立过程中，每个成员总是优先保留自己的成员编号，如果出现冲突，则会按照如下优先级进行分配：

  （1）原来归属于当前 Master 管理的成员优先保留自己的编号；

  （2）编号模式为手动模式的比自动编号模式的优先，手动编号无法得到满足的成员将会更改为自动编号模式；

  （3）成员优先级高的优先；

  （4）MAC 地址小的优先。

  注意：

  1. 可以通过交换机前面板上的成员编号指示灯查看交换机当前的成员编号。
  2. 在堆叠系统运行过程中，手动更改成员编号时，只能更改为尚未使用的编号。

- **端口命名规则**

  端口编号格式为：设备编号/插槽位/端口序号。其中：

  （1）设备编号：缺省情况下，设备编号为 1；如果设备曾经加入过堆叠系统，则在退出堆叠系统后，仍然会使用在堆叠系统中时的成员编号作为自身的设备编号。

  （2）插槽位：此位表示接口卡所在槽位的编号。对于 T3700G-28TQ 系列交换机，主端口的编号为 0，接口模块扩展卡槽位外接扩展卡后其编号值为 1。

  （3）端口序号：端口序号为设备上该端口的编号，具体请查看设备前面板。

  例如：端口编号 2/0/3 表示编号为 2 的设备上的 3 号主端口。

- **配置文件应用规则：**配置文件分为全局配置和端口配置两部分。

  （1）堆叠系统中所有成员设备的全局配置都是相同的，所有成员设备都严格执行 Master 设备当前的全局配置，以保证整个堆叠系统能够像一台设备一样在网络中工作。堆叠系统采用以下方式来保证全局配置文件的同步：

  堆叠系统启动时，当选为 Master 的设备会比较各成员设备的配置文件，并重新配置所有与自己的全局配置不同的设备，以保证整个堆叠系统全局配置的统一。

  堆叠系统正常工作后，用户进行的任何全局配置，都会记录到 Master 设备的当前配置文件中，并同步到堆叠系统中的各个设备。

  （2）各个成员设备都只保存自身的端口配置，用户进行的所有的端口配置也都只保存在相关的成员设备上并执行。

- **堆叠维护**

  堆叠维护的主要功能是监控成员设备的加入和离开，并随时收集新的拓扑，维护现有拓扑。

  在堆叠系统正常运行过程中，成员设备间会不断有数据包的接收和发送。交换机通过监控数据包的响应，可以快速的判断堆叠口的连接状态。当交换机检测到堆叠口的连接状态发生变化时，会重新收集系统拓扑信息并更新拓扑数据库，以保证堆叠系统的正常工作。

导致堆叠口连接状态发生变化从而影响系统拓扑的事件有：成员设备故障或离开、成员设备加入、链路故障或修复等。当 Master 设备故障或离开时，系统会选举出新的 Master 接替原 Master 的工作。

5.1 堆叠的配置

用户配置堆叠前，需要做好前期规划工作，明确堆叠系统内各成员设备的角色和功能。因为有些参数的配置需要重启设备才能生效，所以建议先进行堆叠参数的配置，将设备断电后再进行物理连线，然后上电，设备将自动加入堆叠系统。在堆叠系统形成后，用户通过堆叠系统中的任意一台设备登录，均可以对整个堆叠系统进行配置和管理。

下面分别介绍堆叠的三个配置页面：**堆叠信息**、**堆叠配置**、**堆叠编号**。

5.1.1 堆叠信息

堆叠信息页面主要用于查看堆叠的基本信息。进入界面的方法：**堆叠功能>>堆叠管理>>堆叠信息**

图 5-7 堆叠信息

条目介绍：

- **堆叠配置**

堆叠名称： 显示堆叠系统的一个统一标识。

堆叠 MAC： 显示堆叠对外通信时采用的统一 MAC 地址，一般为 Master 设备的 MAC 地址。

堆叠拓扑： 显示当前堆叠的拓扑类型，Line 表示链形连接，Ring 表示环形连接。

验证模式： 显示建立堆叠的过程中采用的验证方式。

- **成员信息**

编号#： 显示各成员设备的 unit 号。

角色： 显示各成员设备在堆叠中的角色，Master 或者 Slave。

Mac 地址： 显示各成员设备的 MAC 地址，是交换机在堆叠中的唯一标识。

优先级： 显示各成员设备的成员优先级，值越大优先级越高，当选为 Master 的可能性越大。

版本： 显示各成员设备的软件版本。

状态： 显示各成员设备的堆叠状态。

- **堆叠口信息**

堆叠口： 显示堆叠口的编号。

状态： 显示当前堆叠口的状态。

邻居： 显示与该堆叠口直接相邻的成员设备的 unit 号。

5.1.2 堆叠配置

本页面用于配置堆叠的相关参数。进入界面的方法：**堆叠功能>>堆叠管理>>堆叠配置**

图 5-8 堆叠配置

条目介绍：

- **堆叠配置**

堆叠名称： 填写堆叠系统的统一标识。堆叠形成后堆叠名称为 Master 上设置的名称。

验证模式： 选择堆叠口之间建立堆叠时验证报文的模式。

- None：不采用密码验证。
- Simple：简单密码验证。
- MD5：采用 MD5 码验证。

验证密码： 当选择验证模式为 Simple 或 MD5 时使用的密码。

重新输入： 重新输入验证密码，与上面一致。

注意:

设备的成员优先级可以通过命令行进行配置，详细配置方式请查看《命令行手册》。

- **堆叠优先级配置**

编号#： 显示成员设备的 unit 号。

角色： 显示成员设备在堆叠中的角色，Master 或者 Slave。

Mac 地址： 显示成员设备在堆叠中的唯一标识。

优先级： 配置成员设备在 master 选举过程中的优先级，越高越优先。

- **堆叠口配置**

堆叠口： 堆叠口的编号。

状态： 当前堆叠口的状态。

5.1.3 堆叠编号

堆叠运行过程中，使用成员编号来标志和管理成员设备。在一个堆叠系统中，成员编号是唯一的。成员编号可以由系统自动分配，也可手动配置。本页面用于设置成员设备的堆叠编号。

进入界面的方法：**堆叠功能>>堆叠管理>>堆叠编号**

图 5-9 堆叠编号

条目介绍：

- **堆叠编号**

选择： 勾选条目进行设置。

当前编号： 显示交换机当前的成员编号。

角色： 显示成员设备在堆叠中的角色。

指定编号： 设置成员设备编号。

- 自动：选择本项时，交换机将被自动分配一个空闲的编号。
- 1-8: 选中这些选项时，交换机首先尝试获取指定的编号，如果已经被占用则按照自动分配方式对待，从尚未使用的编号中选择。

Mac 地址： 显示成员设备在堆叠中的唯一标识。

堆叠配置步骤：

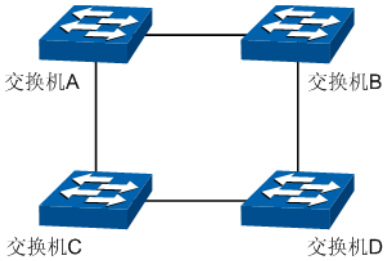
步骤	操作	说明
1	配置堆叠名称	可选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面上配置堆叠名称。默认为 Stack。
2	配置堆叠口模式	必选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面上的堆叠端口配置表中，配置堆叠口的状态为使能（Enable）。
3	配置堆叠验证模式和验证密码	可选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面上配置验证模式和验证密码。
4	配置堆叠成员优先级	可选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面上的堆叠优先级配置表中，配置交换机的成员优先级。
5	配置成员编号	可选操作。在**堆叠功能>>堆叠管理>>堆叠编号**页面上配置交换机的堆叠编号。

5.1.4 组网应用

- **组网需求**

使用 4 台 T3700G-28TQ 交换机建立环形拓扑的堆叠。

- **组网图**



- **配置步骤**

- 在连接拓扑之前先分别配置四台交换机：

步骤	操作	说明
1	设置堆叠名称	可选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面设置堆叠名称。
2	设置堆叠口模式	必选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面中将堆叠端口状态设置为 Enable。
3	设置验证模式及验证密码	可选操作。在**堆叠功能>>堆叠管理>>堆叠配置**页面中选择验证模式，并设置验证密码。
4	配置堆叠编号	可选操作。在**堆叠功能>>堆叠管理>>堆叠编号**页面中分别配置四台交换机的堆叠编号为 1、2、3、4。

- 组成堆叠：

将四台交换机断电后按照组网图连接，然后全部上电，堆叠形成。

回目录

第6章 二层交换

二层交换模块主要用于配置交换机的基本功能，包括**端口管理**、**汇聚管理**、**流量统计**以及**地址表管理**四个部分。

6.1 端口管理

端口管理用于配置交换机端口的基本属性，包括**端口配置**、**端口监控**、**端口安全**、**端口隔离**和**环路监测**五个功能配置页面。

6.1.1 端口配置

端口配置用来配置交换机端口的各项基本参数。端口状态选择“禁用”时，交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

端口基本参数将会直接影响端口的工作方式，请结合实际情况进行配置。

进入页面的方法：二层交换>>端口管理>>端口配置

图 6-1 端口配置

条目介绍：

- **端口配置**

UNIT： 根据UNIT ID选择需要配置的交换机。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

类型： 显示端口的介质类型。

- Copper：表示该端口为普通的RJ45端口。
- SFP：表示该端口为光纤口。
- SFP+：表示该端口为10G光纤口。

描述： 填写端口的描述信息，便于您区分各个端口的用途。

状态： 选择端口状态。只有状态为启用时，端口才能正常转发数据包。

速率双工： 选择端口的传输速率及传输模式。与交换机相连的设备必须与交换机的传输速率及双工状态保持一致。当选择“Auto”选项时，该端口的速率双工由自动协商决定。默认为Auto。

流控： 选择端口的流控状态。启用流控能够同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口状态配置为禁用则不能通过该端口管理交换机，请将要进行管理的端口配置为启用状态。
- 从属于同一个汇聚组的所有成员端口的相应参数配置应该保持一致。

6.1.2 端口监控

端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个或几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。在堆叠系统中，端口监控功能可以对整个堆叠系统的数据进行监控。

进入页面的方法：二层交换>>端口管理>>端口监控

图 6-2 端口监控

条目介绍：

- **监控组列表**

监控组： 显示监控组的组号。

监控端口： 显示每个监控组的唯一的一个监控端口号。

监控方式： 显示每个监控组的监控方式。分为入口监控、出口监控和出入口监控三种方式。

被监控端口： 显示每个监控组的所有被监控端口。

操作： 点击<编辑>按键，对每个监控组的配置进行修改。

点击<编辑>按键，显示界面如下图所示：

图 6-3 监控端口

条目介绍：

- **监控组**

选择组号： 选择要配置的组号。

- **监控端口**

监控端口： 输入监控端口的编号，或者直接在端口选择区选择监控端口。确定监控端口后，需点击右边的<提交>按键保存配置。

- **被监控端口**

UNIT： 根据UNIT ID选择需要进行监控的交换机。

选择： 选择要配置的端口为被监控端口，可多选。

端口：	显示端口号。
入口监控：	选择启用/禁用端口的入口监控功能。端口入口监控功能被启用后，被监控端口收到的数据将复制到监控端口。
出口监控：	选择启用/禁用端口的出口监控功能。端口出口监控功能被启用后，被监控端口发出的数据将复制到监控端口。
LAG：	显示端口当前所属的汇聚组。汇聚组成员端口不能选为监控端口。

注意：

- 汇聚组的成员端口不能作为监控端口。
- 一个端口不可以既作为监控端口又作为被监控端口。
- 端口监控功能可以跨越VLAN进行监控。

6.1.3 端口安全

交换机地址表维护着端口和接入端的MAC地址的对应关系，并以此建立交换路径，地址表的大小是固定的。地址表攻击是指利用工具产生欺骗MAC，快速填满地址表，交换机地址表被填满后，交换机将以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探，攻击获取网络信息。地址表满了后，数据流以洪泛的方式发送到所有端口，会造成交换机负载过大，网络缓慢和丢包甚至瘫痪。

端口安全通过限制端口的最大学习MAC数目，来防范MAC地址攻击并控制端口的网络流量。如果端口启用端口安全功能，将动态学习接入的MAC地址，当学习地址数达到最大值时停止学习。此后，MAC地址未被学习的网络设备将不能再通过该端口接入网络，以保证安全性。

进入页面的方法：二层交换>>端口管理>>端口安全

图 6-4 端口安全

条目介绍：

- **端口安全**

UNIT：	根据UNIT选择需要配置端口安全的交换机。
选择：	勾选端口配置端口安全，可多选。
端口：	显示交换机的端口号。
最大学习地址数：	填写对应端口最多可以学习的MAC地址数目。默认为1024。
已学习地址数：	显示对应端口已经学习的MAC地址数目。
学习模式：	选择MAC地址学习的模式。 ● 动态：MAC地址学习受老化时间的限制，老化时间过后，所学的MAC地址将被删除。 ● 静态：MAC地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目清空。 ● 永久：MAC地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目保持不变。
状态：	选择是否启用端口安全功能。

注意：

- 当端口为汇聚组成员，该端口的端口安全功能被禁用。只有将端口从汇聚组中去掉，才可以使用端口的端口安全功能。
- 若802.1X模块启用，此功能禁用。

6.1.4 端口隔离

通过端口隔离功能，可以为交换机的任意物理端口指定转发端口。设置了端口隔离功能后，每个物理端口只能向自己的转发端口转发数据包。在堆叠系统中，端口隔离可以跨交换机配置。

进入页面的方法：二层交换>>端口管理>>端口隔离

端口隔离列表

UNIT： 1

端口	转发端口
1/0/1	1/0/1-26
1/0/2	1/0/1-26
1/0/3	1/0/1-26
1/0/4	1/0/1-26
1/0/5	1/0/1-26
1/0/6	1/0/1-26
1/0/7	1/0/1-26
1/0/8	1/0/1-26
1/0/9	1/0/1-26
1/0/10	1/0/1-26
1/0/11	1/0/1-26

编辑 帮助

图 6-5 端口隔离列表

条目介绍：

- **端口隔离列表**

可以在主页中查看交换机的端口隔离配置。点击<编辑>按键配置端口隔离，编辑界面如下图所示：

图 6-6 配置端口隔离

条目介绍：

- **端口**

  UNIT： 根据UNIT ID选择要配置端口隔离的交换机，并点击端口区选择物理端口。

- **转发端口**

  UNIT： 根据UNIT ID选择需要隔离的交换机，并点选报文可以被转发到的物理端口。

6.1.5 环路监测

环路监测（Loopback Detection）通过环路监测数据包检测交换机连接的网络中是否存在环路，当检测出环路时根据用户设定处理相应的端口。

进入页面的方法：二层交换>>端口管理>>环路监测

图 6-7 环路监测

条目介绍：

- **全局配置**

环路监测功能： 选择是否启用交换机的环路监测功能。

环路监测间隔： 设置环路监测的时间间隔，默认值为30。

自动恢复时间： 设置被阻塞环路端口的自动恢复时间，设置值为环路监测间隔的整倍数，默认为3。

页面自动刷新： 选择是否启用页面的自动刷新。

自动刷新间隔： 设置页面自动刷新的时间间隔，默认值为3。

- **端口配置**

UNIT： 根据UNIT ID号选择需要进行环路监测的交换机。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用此功能。

处理模式： 选择端口发现环路时的处理模式：

- Alert：端口上发现环路时只发出报警信息。
- Port based：端口上发现环路时发出报警信息，同时阻塞端口。

恢复模式：	选择端口被阻塞后的恢复模式： ● Auto：端口被阻塞后经过自动恢复时间后会自动解除阻塞。 ● Manual：端口被阻塞后只能手动解除阻塞状态。
环路状态：	端口上是否监测到外部环路。
阻塞状态：	端口是否因为监测到环路而处于阻塞状态。
LAG：	显示端口当前所属的汇聚组。
手动恢复：	重置选定端口状态，解除阻塞。

注意：

- 恢复模式设定只对处于非Alert处理模式的端口有效。
- 环路监测务必与风暴抑制配合使用。

6.2 汇聚管理

LAG（Link Aggregation Group，端口汇聚组）是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现流量在汇聚组中各个成员端口之间进行分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括STP、QoS、GVRP、VLAN、端口属性、MAC地址学习等。具体说明如下：

- 开启**IGMP**、**IGMP侦听**、**GVRP**、**802.1Q VLAN**、**语音VLAN**、**生成树**、**QoS配置**、**DHCP侦听**及**端口配置**（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启**端口安全**、**端口监控**、**MAC地址过滤**、**静态MAC地址绑定**、**半双工**、**802.1X认证**、**IP源防护**及**路由端口**功能的端口，不能加入汇聚组。
- 开启**DoS防护**功能的端口，建议不要将其加入汇聚组。

如果您需要配置汇聚组，建议您在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。

说明：

- LAG带宽的计算：当使用四个全双工1000Mbps端口构成LAG时，由于每一个端口上行和下行各是1000Mbps，所以每一个端口的带宽为2000Mbps。它们使用LAG技术汇聚在一起可以形成的最大带宽为8000Mbps。
- LAG的流量会根据选路算法均衡分配到各个成员端口中。当LAG中的一个或几个端口连接断开的时候，这些端口的流量会转移到LAG中其它链接正常的端口中，具备链路冗余备份功能。

按照汇聚方式的不同，端口汇聚可以分为两类：手动配置和LACP配置。本功能包括**汇聚列表**、**手动配置**和**LACP配置**三个配置页面。

6.2.1 汇聚列表

在本页，您可以查看到交换机当前的全部汇聚组。

进入页面的方法：二层交换>>汇聚管理>>汇聚列表

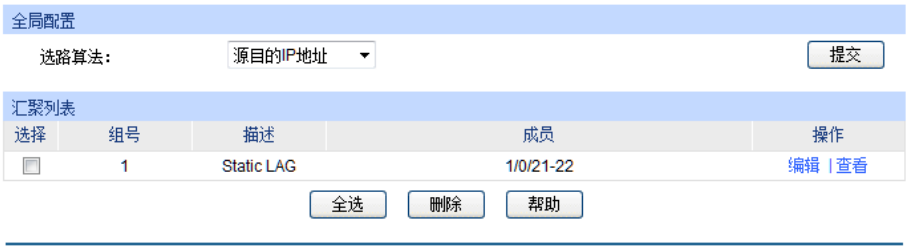


图 6-8 汇聚列表

条目介绍：

- **全局配置**

选路算法： 根据选路算法规则，选择转发数据的端口。

- 源目的MAC地址：仅使用数据包中的源目的MAC地址信息。
- 源目的IP地址：仅使用数据包中的源目的IP地址信息。

- **汇聚列表**

选择： 勾选汇聚组进行删除，可多选。

组号： 显示汇聚组的序号。

描述： 显示汇聚组的描述信息。

成员： 显示属于汇聚组的物理端口。

操作： 对单个汇聚组进行相应配置。

- 编辑：修改汇聚组的描述和成员端口。
- 查看：查看汇聚组的端口状态信息。

点击<查看>按键，您可以看到所选汇聚组的详细信息。

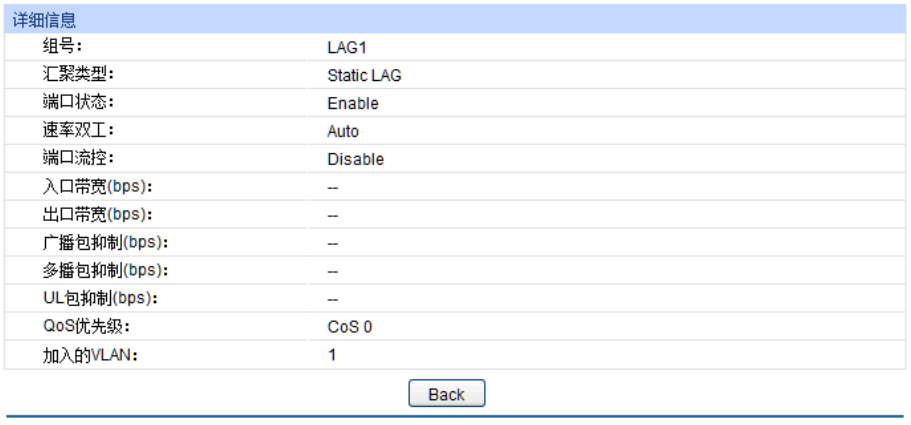


图 6-9 汇聚组状态

6.2.2 手动配置

您可以在本页对汇聚组进行手动配置，手动配置的汇聚端口的LACP状态为禁用。

进入页面的方法：二层交换>>汇聚管理>>手动配置

图 6-10 手动配置

条目介绍：

- **全局配置**

  汇聚组号： 选择汇聚组的序号，组号格式为LAG*。

  汇聚组描述： 显示汇聚组的描述信息。

- **成员端口**

  成员端口： 勾选属于汇聚组的物理端口，清空表示删除该汇聚组。

说明：

- 要删除一个已配置的LAG，将该LAG的成员清空并提交即可。
- 一个端口仅可以处于一个汇聚组中。即若端口已成为其它LAG的成员端口，或者已汇聚成为LACP中的成员时，该端口处于灰化状态，不能勾选。

6.2.3 LACP配置

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是基于 IEEE802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。汇聚的双方通过协议交互汇聚信息，将匹配的链路汇聚在一起收发数据，汇聚组内端口的添加和删除是协议自动完成的，具有很高的灵活性并提供了负载均衡的能力。

启用端口的LACP功能后，该端口向对端通告本端的系统优先级、系统MAC、端口优先级、端口号和操作Key（由端口的物理属性、上层协议信息和管理Key决定）。设备优先级高的一端将主导汇聚及解汇聚，设备优先级由系统优先级和系统MAC决定，系统优先级值小的设备优先级高，系统优先级值相同时系统MAC较小的设备优先级高。设备优先级高的一端将根据端口优先级、端口号以及操作Key选择汇聚端口，操作Key相同的端口才能被选入同一个汇聚组，同一个汇聚组内端口优先级值小的端口会被优先选择，当端口优先级相同的时候，端口号小的会被优先选择。双方交互汇聚信息后被选择的端口将汇聚在一起收发数据。

您可以在本页配置交换机的LACP功能。

进入页面的方法：二层交换>>汇聚管理>>LACP配置

图 6-11 LACP 配置

条目介绍：

- **全局配置**

系统优先级： 与管理Key和系统的MAC地址共同形成链路本端的汇聚标识，即ID。系统优先级的值越小，系统的优先级就越高。不同系统之间交换信息时，具有较高的优先级的系统可以决定一条链路到底属于哪个汇聚链路，而具有较低优先级的系统则根据对方的选择加入合适的汇聚链路。

- **LACP配置**

UNIT： 根据UNIT ID选择需要配置LACP的交换机。

选择： 勾选端口配置端口LACP功能，可多选。

端口： 显示交换机的端口号。

管理Key： 处于同一汇聚组的成员，需配置相同的管理Key。

端口优先级： 决定了成为汇聚组成员的端口的优先级。端口优先级值小的端口会被选择为动态汇聚组成员。若端口优先级相同，则端口号小的会被选择为动态汇聚组成员。默认为32768。

模式： 选择相应端口的LACP模式。

状态： 选择相应端口是否启用LACP功能。

LAG： 显示端口当前所属的汇聚组。

6.3 流量统计

流量统计用于统计流经各个端口的数据信息，本功能包括**流量概览**和**详细统计**两个配置页面。

6.3.1 流量概览

流量概览用来显示交换机各端口的流量信息，便于您监控网络流量和分析网络异常。

进入页面的方法：二层交换>>流量统计>>流量概览

图 6-12 流量概览

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为30秒。

- **流量概览**

UNIT： 根据UNIT ID选择交换机查看具体的流量信息。

端口： 显示交换机的端口号。

接收数据包数： 统计交换机各端口接收的数据包数，不包括错误的数据包。

发送数据包数： 统计交换机各端口发送的数据包数。

接收字节数： 统计交换机各端口接收的字节数，包括错误的数据包的字节数。

发送字节数： 统计交换机各端口发送的字节数。

信息查询： 点击查询相应端口的详细统计信息。

6.3.2 详细统计

详细统计用来统计各端口传输数据包的详细信息，便于您定位网络问题。

进入页面的方法：二层交换>>流量统计>>详细统计

图 6-13 详细统计

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

- **端口选择**

在端口选择区域根据UNIT ID选择交换机，并点选需要查看统计信息的物理端口，点击<确定>按键后下方将显示详细统计信息。

- **详细统计**

端口： 输入您所要查看流量信息的交换机端口号。

接收信息统计： 统计该端口接收数据包的详细信息。

发送信息统计： 统计该端口发送数据包的详细信息。

广播包： 端口接收/发送的含有效广播地址的数据包数目（不含错误帧）。

多播包： 端口接收/发送的含有效多播地址的数据包数目（不含错误帧）。

单播包： 端口接收/发送的含有效单播地址的数据包数目（不含错误帧）。

Alignment错误包： 端口接收的长度为64-10240字节的校验和错误的数据帧数目。

小于64字节包： 端口接收的长度小于64字节的数据帧数目（不含错误帧）。

64字节包： 端口接收的长度为64字节的数据帧数目（包含错误帧）。

65-127字节包： 端口接收的长度为65-127字节的数据帧数目（包含错误帧）。

128-255字节包： 端口接收的长度为128-255字节的数据帧数目（包含错误帧）。

256-511字节包： 端口接收的长度为256-511字节的数据帧数目（包含错误帧）。

512-1023字节包： 端口接收的长度为512-1023字节的数据帧数目（包含错误帧）。

大于1023字节包： 端口接收的长度大于1023字节的数据帧数目（包含错误帧）。

冲突包： 端口工作在半双工模式下发送数据包时产生的冲突包数目。

6.4 地址表管理

交换机的主要功能是对报文进行转发，也就是根据报文的目的MAC地址将报文输出到相应的端口。地址表包含了端口间报文转发的地址信息，是交换机实现报文快速转发的基础。地址表中的表项可以通过自动学习和手动绑定两种方式进行更新和维护，多数地址表条目都是通过自动学习功能来创建和维护的，而对于某些相对固定的连接来说，手动绑定可以提高交换机的效率，通过MAC地址过滤功能可以使交换机对不期望转发的数据帧进行过滤，从而提升了网络安全性。

地址表的分类及特点如下表所示：

地址表类别	配置方式	有无老化时间	重启后是否被保留（配置保存后）	已绑定的MAC地址与端口的关系
静态地址表	手动配置	无	是	在同一VLAN中，已绑定的MAC地址不能被其它端口学习
动态地址表	自动学习	有	否	已绑定的MAC地址可以重新被其它端口学习
过滤地址表	手动配置	无	是	-

本功能包括**地址表显示**、**静态地址表**、**动态地址表**和**过滤地址表**四个配置页面。

6.4.1 地址表显示

在本页可以查看到交换机地址表的全部信息。

进入页面的方法：二层交换>>地址表管理>>地址表显示

图 6-14 地址表显示

条目介绍：

- **显示配置**

  MAC地址： 填写MAC地址查找相应的地址表信息。

  VLAN ID： 填写VLAN ID查找该VLAN学习到的地址表信息。

  地址类型： 选择查看特定的地址类型。

  端口： 选择交换机端口查找该端口学习到的地址条目。

- **地址表**

  UNIT： 根据UNIT ID选择查看指定交换机学习到的地址表。

  MAC地址： 显示交换机学习到的MAC地址。

  VLAN ID： 显示MAC地址条目对应的VLAN ID。

  端口： 显示MAC地址条目对应的交换机端口。

  地址类型： 显示MAC地址的类型。

  老化状态： 显示MAC地址的老化状态。

6.4.2 静态地址表

静态地址表记录了端口上配置的静态地址。静态地址是不会老化的MAC地址，它区别于一般的由端口学习得到的动态地址。静态地址只能手动添加和删除，不受最大老化时间的限制。这对于某些相对固定的连接来说，可减少地址学习步骤，从而提高交换机的转发效率。静态地址表也可以显示在**端口安全**功能中自动学习到的静态MAC地址。

进入页面的方法：二层交换>>地址表管理>>静态地址表

图 6-15 静态地址表

条目介绍：

- **新建条目**

MAC地址： 填写静态绑定的MAC地址。

VLAN ID： 填写MAC地址条目对应的VLAN ID。

端口： 选择静态绑定的交换机端口号。

- **查找条目**

查找选项： 选择静态地址表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：查看静态地址表所有地址信息。
- MAC：填写欲查找条目需包含的MAC地址信息。
- VLAN ID：填写欲查找条目需包含的VLAN ID信息。
- 端口：配置欲查找条目需包含的交换机端口号。

- **静态地址表**

UNIT： 根据UNIT ID选择查看指定交换机的静态地址表信息。

选择： 勾选条目进行删除或修改该条目对应的交换机端口号，可多选。

MAC地址： 显示静态绑定的MAC地址。

VLAN ID： 显示MAC地址条目对应的VLAN ID。

端口： 显示MAC地址条目对应的交换机端口。您可以在此修改与静态MAC地址绑定的端口，但是修改后的端口必须是VLAN的成员端口。

地址类型： 显示MAC地址的类型。

老化状态： 显示MAC地址的老化状态。

注意：

- 如果地址的端口指定错误，或使用过程中端口（或设备）被人为改变，必须重新设置该静态地址表项，否则交换机将无法正确转发数据。
- 静态地址一旦被设置，如果把有此地址的网络设备连接到交换机的其它端口，交换机将不能动态识别。因此必须保证静态地址表中的表项都是正确有效的。
- 凡是加入到静态地址表的地址，不能同时加入到过滤地址表，也不能被端口动态绑定。

6.4.3 动态地址表

动态地址是交换机自动学习的MAC地址，交换机通过自动学习和老化来不断更新其动态地址表。

交换机的地址表的容量是有限的，为了最大限度利用地址表的资源，交换机使用老化机制来更新地址表，即：系统在动态学习地址的同时，开启老化定时器，如果在老化时间内没有再次收到相同地址的报文，交换机就会把该MAC地址从表项删除。

在本页可以配置交换机的动态地址表功能。

进入页面的方法：二层交换>>地址表管理>>动态地址表

图 6-16 动态地址表

条目介绍：

- **老化设置**

  自动老化： 选择是否启用自动老化。

  老化时间： 填写您需要的地址老化时间。默认为300秒。

- **查找条目**

  查找选项： 选择动态地址表的显示规则，可以帮助您快速查找到所需的条目。
  - 全部：查看动态地址表所有地址信息。
  - MAC：填写欲查找条目需包含的MAC地址信息。
  - VLAN ID：填写欲查找条目需包含的VLAN ID信息。
  - 端口：选择欲查找条目需包含的交换机端口号。

➢ **动态地址表**

UINT： 根据UNIT ID选择查看指定交换机的动态地址表信息。

选择： 勾选动态地址条目进行删除或将该条目绑定为静态地址，可多选。

MAC地址： 显示动态绑定的MAC地址。

VLAN ID： 显示MAC地址条目对应的VLAN ID。

端口： 显示MAC地址条目对应的交换机端口号或汇聚组号。

地址类型： 显示MAC地址的类型。

老化状态： 显示MAC地址的老化状态。

绑定： 将动态绑定的地址条目转化为静态绑定。

说明：

- 老化时间过长会导致交换机的地址表中保存过多过时的地址表项，从而耗尽地址表的资源，导致交换机无法根据网络的变化更新地址表。老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。建议您使用默认值。

6.4.4 过滤地址表

通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤，过滤地址不会被老化，只能手工进行添加和删除。在过滤地址表中添加受限的MAC地址后，交换机将自动过滤掉源/目的MAC地址匹配的数据，以保护网络安全。过滤地址表中的地址对所有的交换机端口都生效。

进入页面的方法：二层交换>>地址表管理>>过滤地址表

图 6-17 过滤地址表

条目介绍：

➢ **新建条目**

MAC地址： 填写过滤的MAC地址。

VLAN ID： 填写MAC地址条目对应的VLAN ID。

➢ **查找条目**

查找选项： 选择过滤地址表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：查看过滤地址表所有地址信息。
- MAC：填写欲查找条目需包含的MAC地址信息。
- VLAN ID：填写欲查找条目需包含的VLAN ID信息。

➢ **过滤地址表**

选择： 勾选过滤地址条目进行删除，可多选。

MAC地址： 显示过滤的MAC地址。

VLAN ID： 显示MAC地址条目对应的VLAN ID。

端口号： 此处为"--"，表示无指定端口。

地址类型： 显示MAC地址的类型。

老化状态： 显示MAC地址的老化状态。

注意：

- 已加入到过滤地址表中的地址不能被加入到静态地址表中，也不能被端口动态绑定。
- 若802.1X模块开启，此功能禁用。

回目录

第7章 VLAN

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显着下降甚至使网络不可用等问题。通过交换机实现LAN互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network）技术，这种技术可以把一个LAN划分成多个逻辑的LAN——VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文被限制在一个VLAN内。同一个VLAN内的主机通过传统的以太网通信方式进行报文的交互，而不同VLAN内的主机之间则需要通过路由器或三层交换机等网络层设备进行通信。如图 7-1所示。

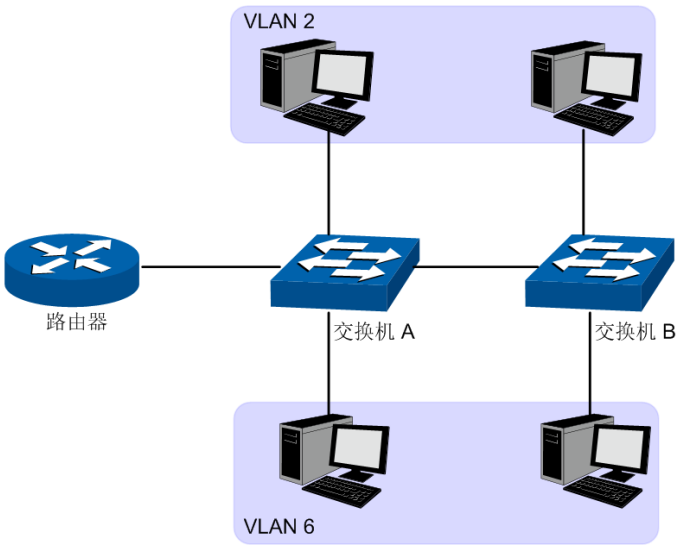


图 7-1 VLAN示意图

VLAN的优点如下：

1) 提高网络性能。将广播包限制在VLAN内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。

2) 增强网络安全。不同VLAN的设备不能互相访问，不同VLAN的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

3) 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

VLAN划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个VLAN；一个VLAN包含的用户可以连接在同一个交换机上，也可以跨越交换机。本交换机支持的VLAN类型有802.1Q VLAN、MAC VLAN和协议VLAN。协议VLAN仅对untag数据包和优先级tag数据包生效。当一个数据包同时满足802.1Q VLAN、MAC VLAN和协议VLAN时，交换机将按照MAC VLAN、协议VLAN、PVID的顺序来处理数据包，在相应VLAN中转发数据包。

7.1 802.1Q VLAN

由于普通交换机工作在OSI模型的数据链路层，若要交换机能够识别不同VLAN的数据包，只能对数据包的数据链路层封装进行VLAN识别。因此，VLAN识别字段被添加到数据链路层封装中。

IEEE 802.1Q协议为了标准化VLAN实现方案，对带有VLAN标识的数据包结构进行了统一规定。协议规定在目的MAC地址和源MAC地址之后封装4个字节的VLAN Tag，用以标识VLAN的相关信息，

如图 7-2所示。VLAN Tag包含四个字段，分别是TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和VLAN ID。

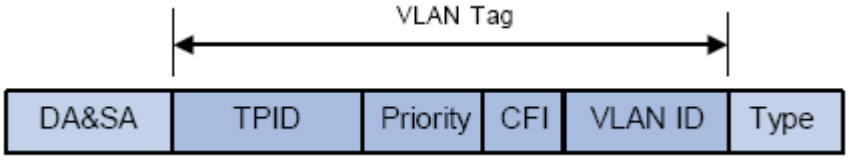


图 7-2 VLAN Tag组成字段

1) TPID：用来表示本数据帧是带有VLAN Tag的数据。该字段长度为16bit。协议规定的缺省取值为0x8100。

2) Priority：用来表示数据包的传输优先级。

3) CFI：以太网交换机中，CFI总被设置为0。由于兼容特性，CFI常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧CFI设置为1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。

4) VLAN ID：用来标识该报文所属VLAN的编号。该字段长度为12bit，取值范围为0~4095。由于0和4095通常不使用，所以VLAN ID的取值范围一般为1~4094。VLAN ID简称VID。

交换机利用VLAN ID来识别报文所属的VLAN，当接收数据包不带VLAN Tag时，交换机会为该数据包封装带有接收端口默认VLAN ID，将数据包在接收端口的缺省VLAN中进行传输。

本手册中，对包含VLAN Tag字段的数据包我们简称为tag帧，untag帧指数据包中没有VLAN Tag字段的数据包，优先级tag帧指数据包中有VLAN Tag字段，但VLAN ID为0的数据包。

- **端口的三种链路类型**

在创建802.1Q VLAN时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

1) ACCESS：端口只能属于1个VLAN，出口规则为UNTAG，多为连接用户终端设备的端口。当ACCESS类型端口加入了其它VLAN时，则自动退出原有VLAN。

2) TRUNK：端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，常用于网络设备之间级连。在网络中VLAN经常跨接在不同交换机上，TRUNK类型端口的默认出口规则为TAG，在转发端口默认VLAN数据时去掉VLAN信息，转发其余VLAN数据时保持原有VLAN信息。

3) GENERAL：端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，可以用于网络设备之间连接，也可以用于连接用户设备。GENERAL类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

- **PVID与VLAN数据包处理关系**

PVID（Port VLAN ID），就是端口的缺省VID。当交换机的端口接收到的报文不带VLAN Tag时，交换机会根据接收端口的PVID值为该报文插入VLAN Tag，并进行转发。

当在局域网中划分VLAN时，PVID是每个端口的一个重要参数，表示端口默认所属的VLAN。它有两个用途：

1) 当端口收到untag报文时，将根据PVID为数据包插入VLAN Tag。

2) PVID指定了端口的默认广播域，即当端口接收到UL包或广播包的时候，交换机将这些数据包在该端口的默认VLAN内广播。

端口的链路类型本质上是交换机对出入端口的VLAN Tag的处理方式，详细规则如表 7-1所示。

端口类型	对接收报文的处理		发送报文时的处理
	报文不带Tag	报文带Tag	
Access	接收报文，并为报文添加缺省的VLAN Tag即输入端口的PVID。	当VID＝端口PVID,接收报文。 当VID≠端口PVID,丢弃报文。	去掉Tag后，发送报文。
Trunk		当VID属于端口允许通过的VLAN ID时，接收报文。 当VID不属于该端口允许通过的VLAN ID时，丢弃报文。	转发端口默认VLAN数据时去tag后发送报文，其余保持原有Tag发送报文。
General			当出口规则配置为TAG时，保持原有tag发送报文。 当出口规则配置为UNTAG时，去tag后发送报文。

表 7-1 端口类型与VLAN数据处理关系

IEEE802.1Q VLAN功能包括**VLAN配置**、**端口配置**两个配置页面。

7.1.1 VLAN配置

在VLAN配置页面中可以查看当前已经创建的802.1Q VLAN。

进入页面的方法：VLAN>>802.1Q VLAN>>VLAN配置

图 7-3 查看VLAN列表

在缺省情况下，为了保证交换机在出厂情况下能正常通信，系统已创建缺省VLAN1，包含所有端口，该VLAN无法删除。

条目介绍：

- **VLAN配置列表**

选择： 勾选条目进行删除，可多选。

VLAN ID： 显示VLAN ID。

名称： 显示VLAN的描述信息。

成员： 显示VLAN的端口成员。

操作： 对单个VLAN条目进行相应操作。

- 编辑：修改VLAN配置。
- 详细：查看VLAN配置信息。

点击<编辑>按键，可以对相应的VLAN进行编辑。点击<新建>按键，可以创建新的VLAN。

图 7-4 创建或编辑802.1Q VLAN

条目介绍：

- **VLAN配置**

VLAN ID：	填写VLAN ID。
VLAN名称：	填写VLAN的描述信息，以便区分各个VLAN的用途。
Untagged端口：	点选当前配置的VLAN包含的Untagged端口，指定端口在转发该VLAN的数据时将去掉tag信息。
Tagged端口：	点选当前配置的VLAN包含的Tagged端口，指定端口在转发该VLAN的数据时将加上tag信息。

7.1.2 端口配置

在创建802.1Q VLAN时，需要对端口连接的设备进行了解，以便设置各端口的参数。

进入页面的方法：**VLAN>>802.1Q VLAN>>端口配置**

图 7-5 802.1Q VLAN—端口配置

条目介绍：

- **VLAN端口配置**

UNIT： 根据UNIT ID选择需要配置的交换机。

选择： 勾选端口配置端口类型和PVID值，可多选。

端口： 显示交换机的端口号。

端口类型： 选择交换机的端口类型。默认为ACCESS。

- ACCESS：该端口只能加入一个VLAN，出口规则为UNTAG。如果VLAN删除，相应端口的PVID会自动置为默认值1。
- TRUNK：该端口可加入多个VLAN，转发端口默认VLAN数据时出口规则为UNTAG，转发其余VLAN数据时出口规则为TAG。
- GENERAL：该端口可加入多个VLAN，且允许根据不同VLAN选择不同的出口规则，默认出口规则为UNTAG。

PVID： 配置端口的默认VLAN ID。当端口接收到UNTAG数据时，将在端口默认VLAN中转发。ACCESS类型端口不能设置PVID，默认与端口所属VLAN ID保持一致。

LAG： 显示端口当前所属的汇聚组。

所属VLAN： 查询本端口所加入的VLAN信息。

点击<查询>按键，可以查询相应端口的所属VLAN。点击<移除>按键，即可将端口从相应VLAN删除。

图 7-6 查看端口所属VLAN

802.1Q VLAN配置步骤：

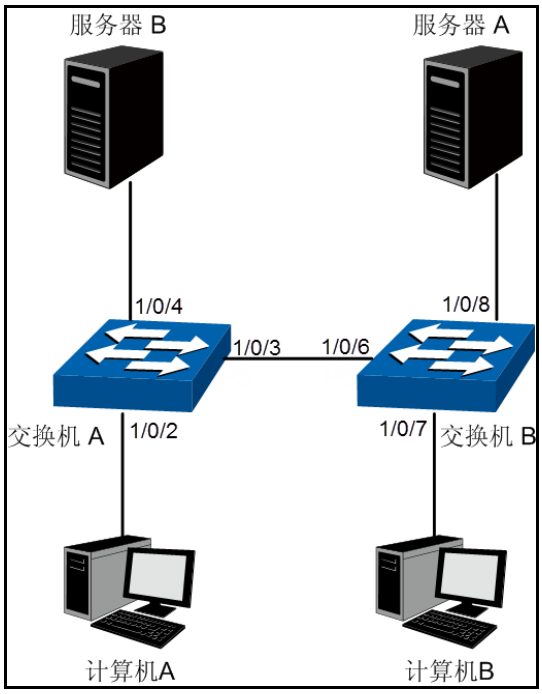
步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建VLAN	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，请输入VLAN ID并对其进行描述，在此页面中请同时勾选VLAN包含的Tagged端口和Untagged端口。
3	编辑/查看VLAN	可选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面点击<编辑>或<查看>按键，可以对相应的VLAN进行编辑和查看。
4	删除VLAN	可选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面勾选相应的VLAN条目，点击<删除>按键进行删除。

7.2 802.1Q VLAN功能的组网应用

- **组网需求**

- 交换机A连接了计算机A和服务器B；
- 交换机B连接了计算机B和服务器A；
- 计算机A和服务器A同属于一个部门；
- 计算机B和服务器B同属于一个部门；
- 两个部门以VLAN划分，相互之间不能通信。

➢ **组网图**



➢ **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/2的类型为ACCESS；设置端口1/0/3的类型为TRUNK；端口1/0/4类型为ACCESS。
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，并包含的Untagged端口1/0/2和Tagged端口1/0/3。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，并包含的Tagged端口1/0/3和Untagged端口1/0/4。

- 配置交换机B：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/7的类型为ACCESS；设置端口1/0/6的类型为TRUNK；端口1/0/8类型为ACCESS。
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，并包含的Tagged端口1/0/6和Untagged端口1/0/8。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，并包含的Tagged端口1/0/6和Untagged端口1/0/7。

7.3 MAC VLAN

MAC VLAN是VLAN的另一种划分方法，根据每个主机的MAC地址来划分VLAN，即对每个主机的MAC地址均划分到VLAN中。MAC VLAN的优点在于，将MAC地址与VLAN绑定后，该MAC地址对应的设备可以随意切换端口，只要连接到相应VLAN的成员端口即可，而不必改变VLAN成员的配置。

MAC VLAN 中数据包处理有如下特点：

1. 当端口收到 UNTAG 数据包时，首先查看是否创建配置相应的 MAC VLAN，若已创建 MAC VLAN，则给数据包插入 MAC VLAN 的 TAG；若没有相应的 MAC VLAN，则根据接收端口的 PVID 值给数据包插入 TAG，并将数据包在相应的 VLAN 中转发。
2. 当端口收到 TAG 数据包时，交换机按照 802.1Q VLAN 的方式处理该帧。如果接收端口允许该 VLAN 的数据包通过，则正常转发；如果不允许，则丢弃该数据包。

将某个主机的 MAC 划分到 802.1Q VLAN 中后，为了保证该主机能够在此 VLAN 内正常通信，请将其接入端口设置成相应的 802.1Q VLAN 成员。详情请查看表 7-1。

7.3.1 MAC VLAN

在 MAC VLAN 页面中，可以创建 MAC VLAN 并查看当前已创建的 MAC VLAN。

进入页面的方法：VLAN>>MAC VLAN>>MAC VLAN

图 7-7 创建并查看 MAC VLAN

条目介绍：

- **MAC VLAN 配置**

  MAC 地址： 输入 MAC 地址。

  MAC 描述： 输入对 MAC 地址的描述，以便区分各个 MAC 的用途。

  VLAN ID： 输入该 MAC VLAN 对应的 VLAN ID，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

- **MAC VLAN 列表**

  MAC 地址选择： 点击<选择>按键，可根据所输 MAC 快速查找 MAC VLAN 条目。

  选择： 勾选条目进行删除，可多选。

MAC 地址：	显示 MAC 地址。
MAC 描述：	显示此 MAC 的描述信息，以便区分各个 MAC 的设备。
VLAN ID：	显示该 MAC 对应的 VLAN ID。
操作：	点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

7.3.2 端口使能

端口使能用来开启端口的 MAC VLAN 功能。只有配置了 MAC VLAN 并使能端口，才能正式启用 MAC VLAN 功能。

进入页面的方法：VLAN>>MAC VLAN>>端口使能

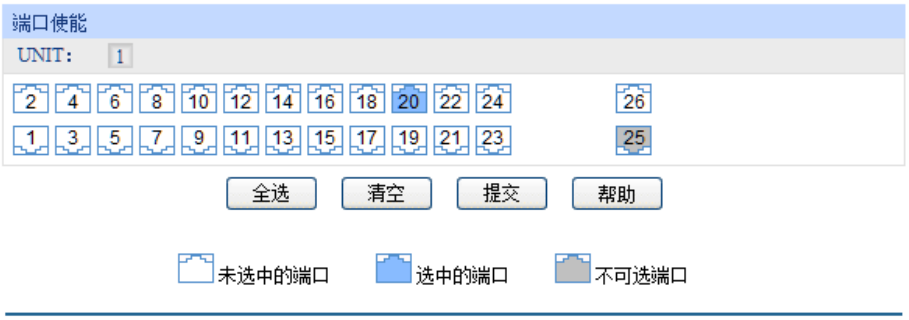


图 7-8 端口使能 MAC VLAN 特性

条目介绍：

- **端口使能**

根据 UNIT ID 切换交换机，并点选特定端口配置端口的 MAC VLAN 特性，选中端口并提交保存后，端口将使能 MAC VLAN 特性。当前显示蓝色的端口表示已经使能 MAC VLAN 特性。

MAC VLAN 配置步骤：

步骤	操作	说明
1	创建 MAC VLAN	必选操作。在 **VLAN>>MAC VLAN>>MAC VLAN** 页面创建 MAC VLAN。创建了 MAC VLAN 后，对应 MAC 地址的设备在交换机上的连接端口也必须是 VLAN 成员，才能保证正常通信。
2	端口使能	必选操作。在 **VLAN>>MAC VLAN>>端口使能**页面选择需要使能 MAC VLAN 特性的端口，点击<提交>使设置生效。

7.4 协议VLAN

协议VLAN是按照网络层协议来划分VLAN，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。这种按网络层协议来组成的VLAN，可使广播域跨越多个交换机，同时用户在网络内部可以自由移动且无须改变其VLAN成员身份。对于希望针对具体应用和服务来管理用户的网络管理员，可通过划分协议VLAN来进行管理。

本交换机可针对常见的协议类型划分VLAN，常用协议类型值见下表。请根据实际需要创建协议VLAN。

协议类型	对应取值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表 7-2 常用协议类型

协议VLAN中数据包处理有如下特点：

1. 当端口收到UNTAG数据包时，首先查看是否创建配置相应的协议VLAN，若已创建协议VLAN，则给数据包插入协议VLAN的TAG；若没有相应的协议VLAN，则根据接收端口的PVID值给数据包插入TAG，并将数据包在相应的VLAN中转发。
2. 当端口收到TAG数据包时，交换机按照802.1Q VLAN的方式处理该帧。如果接收端口属于携带该VLAN TAG的数据包通过，则正常转发；如果不属于，则丢弃该数据包。

划分了协议VLAN后，为了保证数据的正常传输，请将协议VLAN的使能端口设置为相应802.1Q VLAN成员。详情请查看表 7-1。

7.4.1 协议组列表

本页面中可以查看当前交换机上配置的协议VLAN，同时可以删除或编辑协议VLAN。

进入页面的方法：VLAN>>协议VLAN>>协议组列表

图 7-9 协议VLAN列表

条目介绍：

- **协议组列表**

选择： 勾选条目进行删除，可多选。

协议类型： 显示协议VLAN的协议类型。

VLAN ID： 显示该协议对应的VLAN ID。

成员： 显示该协议组成员的端口号。

操作：	点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<提交>按键，使修改内容生效。

7.4.2 协议组配置

在协议组配置页面中，可以创建协议VLAN。

进入页面的方法：VLAN>>协议VLAN>>协议组配置

图 7-10 创建并查看协议 VLAN

条目介绍：

- **协议组配置**

协议类型：	选择交换机已定义的协议模板。
VLAN ID：	输入协议VLAN ID。
协议组成员：	根据UNIT ID选择指定的交换机，并点选端口作为协议VLAN的成员端口。

7.4.3 协议模板

配置协议VLAN前应先配置协议模板，本交换机在出厂默认情况下已经定义了IP、ARP和RARP等协议模板，若需要更多的协议模板时，请在此页面中添加。

进入页面的方法：**VLAN>>协议VLAN>>协议模板**

图 7-11 创建并查看协议模板

条目介绍：

- **协议模板配置**

  协议类型： 配置新定义的协议模板的名称。

  帧类型： 选择该协议模板针对的数据帧类型，本交换机能够识别Ethernet II、SNAP、LLC三种数据帧类型。

  以太网类型： 当配置的帧类型选择为Ethernet II或SNAP类型时，需定义具体的以太网协议类型值。

  DSAP/SSAP： 当配置的帧类型选择为LLC类型时，需定义具体的DSAP域和SSAP域值。

- **协议模板列表**

  选择： 勾选条目进行删除，可多选。

  协议类型： 显示协议模板的名称。

  协议类型： 显示该协议模板中的帧类型。

注意：

- 当协议模板与VLAN绑定后，将无法删除协议模板。

协议VLAN配置步骤：

步骤	操作	说明
1	创建协议模板	必选操作。配置协议VLAN前应先在**VLAN>>协议VLAN>>协议模板**页面配置协议模板。
2	创建协议VLAN并使能端口	必选操作。在**VLAN>>协议VLAN>>协议组配置**页面中选择协议类型并输入VLAN ID来创建VLAN，同时选择支持协议VLAN的端口。

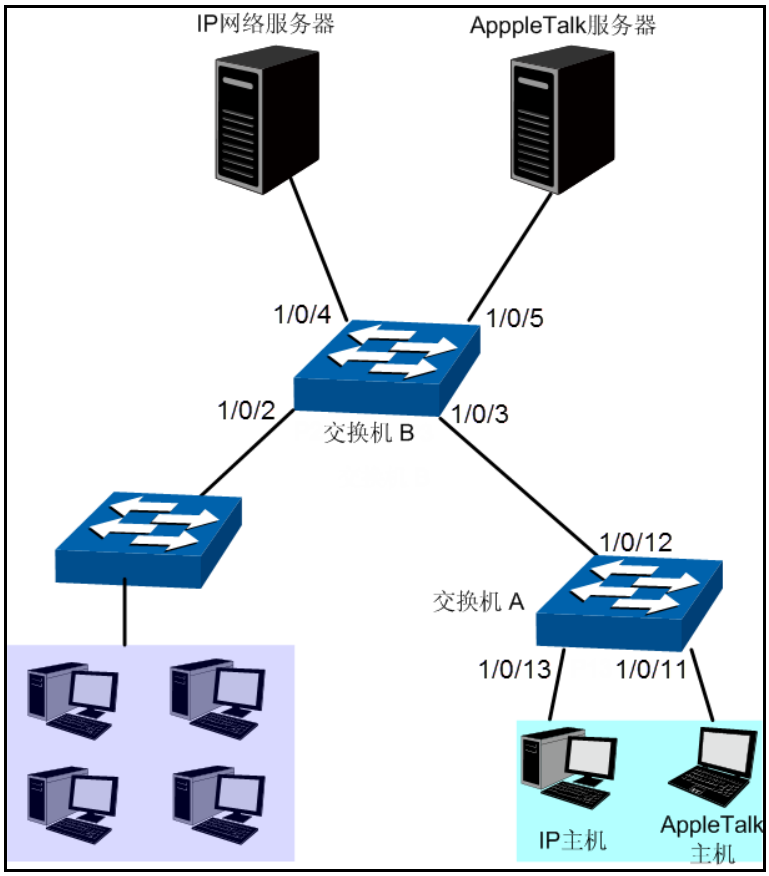
步骤	操作	说明
3	编辑/查看VLAN	可选操作。在**VLAN>>协议VLAN>>协议组列表**页面点击<编辑>按键对相应的VLAN进行编辑。
4	删除VLAN	可选操作。在**VLAN>>协议VLAN>>协议组列表**页面勾选相应的VLAN条目，点击<删除>按键进行删除。

7.5 协议 VLAN 功能的组网应用

➢ **组网需求**

- 平面部门通过内部交换机A的端口1/0/12连入公司局域网；
- 平面部门中分别有IP主机和AppleTalk主机；
- IP主机需要IP网络服务器提供服务，属于VLAN10；AppleTalk主机需要AppleTalk服务器提供服务，属于VLAN20；
- 交换机A分别连接了IP网络服务器和AppleTalk网络服务器；

➢ **组网图**



➢ **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/11和端口1/0/13的端口类型为ACCESS，端口12的端口类型为GENERAL。

步骤	操作	说明
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，包含Untagged端口1/0/12和1/0/13。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，包含Untagged端口1/0/11和端口1/0/12。

- 配置交换机B：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/4和端口1/0/5的端口类型为ACCESS，端口1/0/3的端口类型为GENERAL。
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，包含Tagged端口1/0/3和Untagged端口1/0/4。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，包含Tagged端口1/0/3和Untagged端口1/0/5。
4	创建协议模板	必选操作。此处请根据实际情况在**VLAN>>协议VLAN>>协议模板**页面配置协议模板。例如IP网络数据包以Ethernet II类型封装，Ether Type字段为0800；AppleTalk网络数据包以SNAP类型封装，PID字段为809B。
5	设置协议VLAN 10	在**VLAN>>协议VLAN>>协议组列表**页面中点击<新建>按键来创建协议VLAN10，关联IP协议，并勾选成员端口1/0/3。
6	设置协议VLAN 20	在**VLAN>>协议VLAN>>协议组列表**页面中点击<新建>按键来创建协议VLAN20，关联AppleTalk协议，并勾选成员端口1/0/3。

7.6 VLAN VPN

VPN（Virtual Private Network，虚拟私有网络）是随着Internet的广泛应用而迅速发展起来的一种新技术，用来实现在骨干网络上构建私人专用网络。通过在客户端或运营商接入端对指定报文进行处理，使骨干网络中的设备可以为其建立专用的传输隧道，保证数据的安全。

VLAN-VPN(Virtual Private Network)是一种简单、灵活的二层VPN技术，它通过在运营商接入端为用户的私网报文封装外层VLAN Tag，使报文携带两层VLAN Tag穿越运营商网络（骨干网）。在骨干网中，报文只根据外层VLAN Tag进行传输，用户的私网VLAN Tag则当作报文中的数据部分来进行传输。

VLAN-VPN主要可以解决如下几个问题：

（1） 为小型城域网或企业网提供一种较为简单的二层VPN解决方案。

（2） 缓解日益紧缺的公网VLAN ID资源问题。

（3） 用户可以规划自己的私网VLAN ID，不会导致和骨干网VLAN ID冲突。

（4） 当运营商升级网络时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

➢ 我司交换机VLAN-VPN实现方式

在本交换机中，将用户的原始VLAN称作C VLAN；而骨干网络中，运营商通常使用公网VLAN为不同的C VLAN提供服务，本交换机中将公网VLAN称为SP VLAN。在本交换机上，需要在入口端配置端口PVID为运营商的公网VLAN，并使能端口VLAN VPN功能，连接公网的端口设置为上联端口，使报文顺利穿越骨干网络到达目的地。

1. 当启用VLAN-VPN功能时，需要同时使能端口的VLAN VPN功能。启用VLAN-VPN功能后，不管端口收到tagged或者untagged报文，交换机都会根据PVID给报文封装外层VLAN Tag，然后通过上联端口在骨干网络中传输双Tag报文。
2. 如果开启了VLAN-VPN功能，为了保证报文能够在骨干网络中进行传输，请将连接到骨干网络的端口设置为上联端口。
3. 同时，本交换机还支持TPID值可调功能。TPID（Tag Protocol Identifier，标签协议标识）是VLAN Tag中的一个字段，IEEE802.1Q协议规定该字段的取值为0x8100。本交换机缺省采用协议规定的TPID值（0x8100）。某些厂商将网络设备可识别的TPID值设置为0x9100或其它数值。为了和这些设备兼容，本交换机提供了全局的VLAN-VPN报文TPID值可调功能，用户可以自行配置TPID值。VLAN-VPN上联端口在转发报文时会将报文外层VLAN Tag中的TPID值替换为设定值再进行发送，从而使发送到骨干网中的VLAN-VPN报文可以被其它厂商的设备识别。

   由于TPID字段在以太网报文中的位置与不带VLAN Tag的报文中协议类型字段所处位置相同，为避免网络中报文转发和接收造成混乱，用户在配置VLAN-VPN时，请勿配置TPID为表 7-3中列举的常用协议类型值。

协议类型	对应取值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表 7-3 常用以太网数据包协议类型值

本功能包括**VPN配置**、**端口使能**和**VLAN映射**三个配置页面。

7.6.1 VPN配置

在VPN配置页面中，可以启用交换机VPN功能、设置全局TPID值和启用上联端口。启用VPN模式后，交换机将根据VLAN映射表条目对接收数据包的tag标识插入外层tag。

进入页面的方法：VLAN>>VLAN VPN>>VPN配置

图 7-12 VPN 全局功能配置

条目介绍：

- **VPN全局配置**

  VPN模式： 选择是否启用VLAN-VPN功能。

  全局TPID： 填写全局TPID。

- **VPN上联端口**

勾选端口设置为VPN上联端口，请将连接到骨干网络的端口设置为上联端口。

7.6.2 端口使能

端口使能用来开启端口的VLAN VPN功能。只有在使能端口之后，才能正式启用VLAN VPN功能。

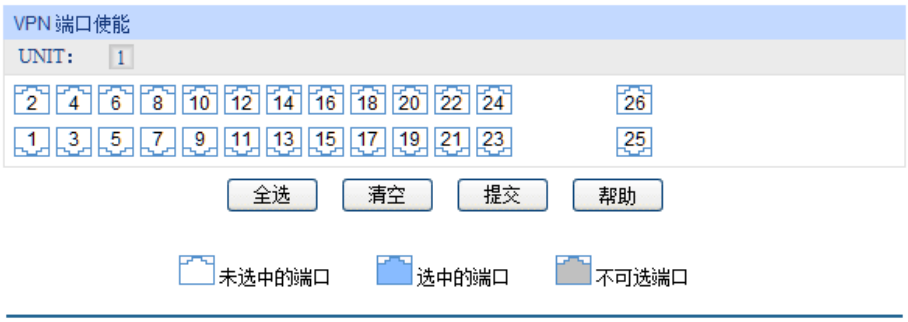


图 7-13 使能端口

勾选端口使能端口的VLAN VPN功能，默认情况下关闭所有端口的VLAN VPN功能。

7.6.3 VLAN映射

VLAN映射页面可以配置基于端口的C_VLAN和SP VLAN的映射关系，VLAN VPN功能将按照VLAN映射条目加上外层VLAN TAG，然后交换机在新的VLAN范围内转发报文。

进入页面的方法：**VLAN>>VLAN VPN>>VLAN映射**

图 7-14 VLAN 映射配置

条目介绍：

- **VLAN映射配置**

VLAN映射：	启用或禁用全体VLAN映射列表。如果没有使能VLAN映射列表，VLAN VPN功能将根据数据接收端口的PVID值为数据加入外层TAG后转发。

- **VLAN映射配置**

端口：	选择VLAN映射功能的生效端口，只有指定端口在收到C_VLAN标识的数据时才加上外层SP VLAN标识再转发。
C_VLAN：	Customer VLAN ID，数据的源VLAN。
SP VLAN：	Service Provider VLAN ID，数据的Tag标识字段将被加上SP VLAN标识。
名称：	为相应的VLAN映射条目定义名称。

- **VLAN映射列表**

在该表格中查看交换机上当前已配置的VLAN映射表。

VLAN VPN配置步骤：

步骤	操作	说明
1	设置全局VLAN VPN参数	必选操作。在**VLAN>>VLAN VPN>>VPN配置**功能页面，启用VPN模式功能，根据对端设备属性设置全局TPID值，并启用VPN上联端口。请将连接到骨干网络的端口设置为上联端口。
2	设置端口使能	必选操作。在**VLAN>>VLAN VPN>>端口使能**功能页面，配置端口使能VLAN VPN特性。
3	设置VLAN映射关系	必选操作。在**VLAN>>VLAN VPN>>VLAN映射**功能页面，配置C VLAN和SP VLAN的映射关系。

7.7 GVRP

GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。

- **GARP简介**

GARP提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息。GARP本身不作为一个实体存在于设备中，遵循GARP协议的应用实体称为GARP应用，GVRP就是GARP的一种应用。当GARP应用实体存在于设备的某个端口上时，该端口称为GARP应用实体。

网络中的GARP应用实体之间通过传递GARP消息来完成相关的信息交换，GARP协议定义有三类消息，分别为Join消息、Leave消息和LeaveAll消息，三种消息完成相关属性信息的注册或注销。

Join消息：当一个GARP应用实体希望其它设备注册自己的属性信息时，它将对外发送Join消息；当收到其它实体的Join消息或本设备静态配置了某些属性，需要其它GARP应用实体进行注册时，它也会向外发送Join消息。

Leave消息：当一个GARP应用实体希望其它设备注销自己的属性信息时，它将对外发送Leave消息；当收到其它实体的Leave消息注销某些属性或静态注销了某些属性后，它也会向外发送Leave消息。

LeaveAll消息：每个GARP应用实体启动后，将同时启动LeaveAll定时器。当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，LeaveAll消息用来注销所有的属性，以使其它GARP应用实体重新注册本实体上所有的属性信息。

通过消息交互，所有待注册的属性信息可以传播到同一局域网中的所有GARP应用实体。

GARP消息发送的时间间隔通过定时器来控制。GARP协议定义了四种定时器，用于控制GARP消息的发送周期：

Hold定时器：当GARP应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条Join消息对外发送，而是启动Hold定时器，当该定时器超时后，GARP应用实体将此时段内收到的所有注册信息放在同一个Join消息中向外发送，从而节省带宽资源。

Join定时器：GARP应用实体可以通过将每个Join消息向外发送两次来保证消息的可靠传输，在第一次发送的Join消息没有得到回复的时候，GARP应用实体会第二次发送Join消息。两次Join消息发送之间的时间间隔用Join定时器来控制。

Leave定时器：当一个GARP应用实体希望注销某属性信息时，将对外发送Leave消息，接收到该消息的GARP应用实体启动Leave定时器，如果在该定时器超时之前没有收到Join消息，则注销该属性信息。

LeaveAll定时器：每个GARP应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，以使其它GARP应用实体重新注册本实体上所有的属性信息。随后再启动LeaveAll定时器，开始新的一轮循环。

- **GVRP简介**

GVRP是GARP的一种应用。它基于GARP的工作机制，维护设备中的VLAN动态注册信息，并传播VLAN信息到其它设备中。

设备启动GVRP特性后，能够接收来自其它设备的VLAN注册信息，并动态更新本地的VLAN注册信息，包括当前的VLAN成员、这些VLAN成员可以通过哪个端口到达等；同时设备能够将本地的VLAN注册信息向其它设备传播，以便使同一局域网内所有设备的VLAN信息一致。GVRP传播的VLAN注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

在本交换机中，只有TRUNK类型端口才能作为GVRP应用实体，维护交换机的VLAN注册信息。GVRP的端口注册模式有三种：Normal、Fixed和Forbidden，各模式描述如下：

Normal模式： 允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。

Fixed模式：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。Fixed模式的端口只允许本端口所属的静态VLAN信息通过。

Forbidden模式： 禁止该端口动态注册、注销VLAN，不传播除VLAN1以外的任何的VLAN信息。Forbidden模式的端口，只允许系统默认VLAN（VLAN1）通过。

进入页面的方法：VLAN>>GVRP>>GVRP配置

图 7-15 配置GVRP

注意：

- 若启用了LAG组成员端口的GVRP功能，请保持所有成员端口的状态和注册模式一致。

条目介绍：

- **全局配置**

  GVRP功能： 选择是否启用交换机的GVRP功能。

- **端口配置**

  UNIT： 根据UNIT ID选择指定交换机配置其端口的GVRP参数。

选择： 勾选端口，配置端口GVRP功能参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用此功能。端口启用GVRP功能之前需要将端口类型设置为Trunk。

注册模式： 选择端口的注册模式。

- Normal模式：允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。
- Fixed：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。
- Forbidden：禁止该端口动态注册、注销VLAN，只允许缺省VLAN通过。

LeaveAll定时器： 每个端口启动GARP后，同时启动LeaveAll定时器，端口将对外循环发送LeaveAll消息，以使其它端口重新注册其所有的属性信息。LeaveAll定时器的取值范围为1000-30000厘秒。

Join定时器： GARP端口可以将每个Join数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用Join定时器来控制。Join定时器的取值范围为20-1000厘秒。

Leave定时器： 接收到Leave数据包的GARP端口启动Leave定时器，如果在该定时器超时之前没有收到Join数据包，则注销相应属性信息。Leave定时器的取值范围为60-3000厘秒。

LAG： 显示端口当前所属的汇聚组。

注意：

- LeaveAll定时器要大于等于10倍Leave定时器，而Leave定时器要大于等于2倍Join定时器。

GVRP配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面将端口类型设置为TRUNK。
2	启用GVRP功能	必选操作。在**VLAN>>GVRP>>GVRP配置**页面启用GVRP功能。
3	配置端口的注册模式以及各定时器时长。	必选操作。在**VLAN>>GVRP>>GVRP配置**页面中根据实际应用情况设置端口的参数并启用端口。

7.8 Private VLAN

Private VLAN功能采用了分层结构，将多个Secondary VLAN与一个Primary VLAN组成VLAN对，下层用户通过Secondary VLAN相互之间进行二层报文隔离，上层设备仅需识别Primary VLAN从而节约了VLAN资源，解决了上层设备VLAN资源短缺以及传统VLAN中的广播问题。

在园区网和企业接入网中，为了保证用户信息安全，要求对接入用户进行认证接入并相互隔离，通过VLAN进行隔离是最常见的隔离方式。随着接入用户的数量日益增长，用传统VLAN的隔离方式将消耗大量的VLAN资源，上层设备为了识别所有的VLAN，不得不建立数量庞大的VLAN。然而，根据IEEE 802.1Q协议标准定义的4个字节的VLAN Tag，其中12bits用于表示VLAN ID，这也就限制的

网络设备可识别的VLAN数最多为4094个。在VLAN资源消耗殆尽的情况下，Private VLAN功能应运而生，常用网络模型如下图 7-16示。

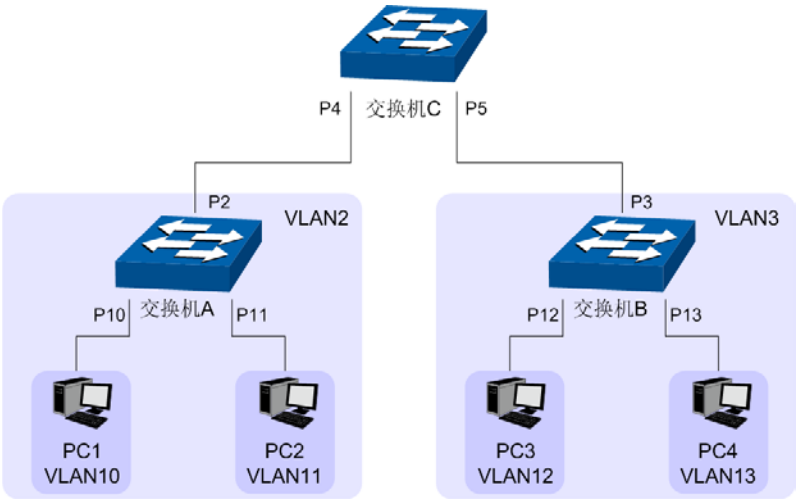


图 7-16 Private VLAN 网络模型

在图 7-16中，交换机A和交换机B分别运用Private VLAN功能，建立Secondary VLAN将终端相互隔离，并将Secondary VLAN与Primary VLAN组成VLAN对，上层设备交换机C只需识别Primary VLAN。

- **我司交换机的Private VLAN实现方式**

Private VLAN功能基于802.1Q VLAN建立Primary VLAN和Secondary VLAN的包含关系，通过这种包含关系，上联设备只需识别Primary VLAN信息，下联设备只需识别Secondary VLAN信息。

Primary VLAN：上行设备感知的用户VLAN，不是用户真正所属的VLAN，一个Primary VLAN可以和多个Secondary VLAN建立包含关系，用于转发上层设备和Secondary VLAN之间的通信数据。

Secondary VLAN：用户真正属于的VLAN，将用户划分到不同的Secondary VLAN中，Secondary VLAN之间相互隔离。

Secondary VLAN有两种类型，Community VLAN和Isolated VLAN。Community VLAN中的成员相互之间可以直接通信，Isolated VLAN中的成员相互隔离。

- **Private VLAN配置要点**

如图 7-16示，以图中的交换机A为例介绍我司交换机的Private VLAN功能，以下为功能配置要点。

（1） 交换机A建立Private VLAN 2/10（Primary VLAN为VLAN 2，Secondary VLAN为VLAN10，下面格式同此处）和Private VLAN 2/11。

（2） 交换机A的端口1/0/10和端口1/0/11作为Host类型端口连接终端用户，分别加入不同的Private VLAN，通过不同的Secondary VLAN相互之间进行隔离。端口1/0/2作为Promiscuous类型端口连接上层设备，通过Primary VLAN 2向上层设备交换机C屏蔽本交换机上的Secondary VLAN的信息。

（3） 交换机A内部执行端口同步机制。创建了Private VLAN 2/10和Private VLAN 2/11后，端口1/0/10和端口1/0/11同时成为Primary VLAN 2的成员端口，端口PVID为各自所属的Secondary VLAN，出口规则为UNTAG；端口1/0/2连接上层设备，同时也同步到Secondary VLAN中成为VLAN成员端口，PVID为Primary VLAN ID，出口规则为UNTAG。

本功能配置简单，包括**PVLAN配置**和**端口配置**两个配置页面。

7.8.1 PVLAN配置

在PVLAN配置页面中，可以创建Private VLAN，将Primary VLAN和Secondary VLAN关联。

进入页面的方法：VLAN>>Private VLAN>>PVLAN配置

图 7-17 PVLAN 配置

条目介绍：

- **Private VLAN创建**

  Primary VLAN： 填写Primary VLAN ID。一个Primary VLAN可以和多个Secondary VLAN关联组成多个Private VLAN。

  Secondary VLAN： 填写Secondary VLAN ID。一个Secondary VLAN中只能和一个Primary VLAN关联，即加入一个Private VLAN。

  Secondary VLAN： 配置Secondary VLAN类型。
  - Community: Secondary VLAN中的成员之间可以互相通信。
  - Isolated: Secondary VLAN中的成员之间相互隔离，不能通信。

- **查找条目**

  查找选项： 当创建的Private VLAN数过多时，可通过指定的Primary VLAN或Secondary VLAN查找相应的Private VLAN条目。

- **Private VLAN列表**

  选择： 勾选条目进行删除或修改交换机Private VLAN配置信息，可多选。

  Primary VLAN： 显示Private VLAN的Primary VLAN ID。

  Secondary VLAN： 显示Private VLAN的Secondary VLAN ID。

  VLAN类型： 显示Secondaty VLAN类型。

  端口成员： 显示Private VLAN的成员端口。当在Private VLAN列表区中修改Private VLAN参数时，其原有的成员端口参数将失效，请重新配置。

7.8.2 端口配置

在本页面中，可以根据端口在网络中的连接状态配置端口类型，并将端口添加到Private VLAN中。

进入页面的方法：VLAN>>Private VLAN>>端口配置

图 7-18 端口配置

条目介绍：

- **端口配置**

  选择的端口： 在端口选择区根据UNIT ID选择指定交换机的端口。

  端口类型： 选择端口类型。
  - Promiscuous：和上行设备相连，负责和上行设备通信。
  - Host：和下行设备相连，负责和下行设备通信。

  Primary VLAN： 填写该端口加入的Primary VLAN。

  Secondary VLAN： 填写该端口加入的Secondary VLAN。

- **Private VLAN端口列表**

  UNIT： 根据UNIT ID查看指定交换机的端口参数。

  端口号： 显示Private VLAN的端口号。

  端口类型： 显示端口在Private VLAN中的端口类型。

  操作： 删除Private VLAN的成员端口。

注意：

- 如果需要把Promiscuous端口加入多个Private VLAN中且Primary VLAN相同时，只需把Promiscuous端口加入任意一个Private VLAN即可，端口将自动同步到其它Private VLAN。

Private VLAN配置步骤：

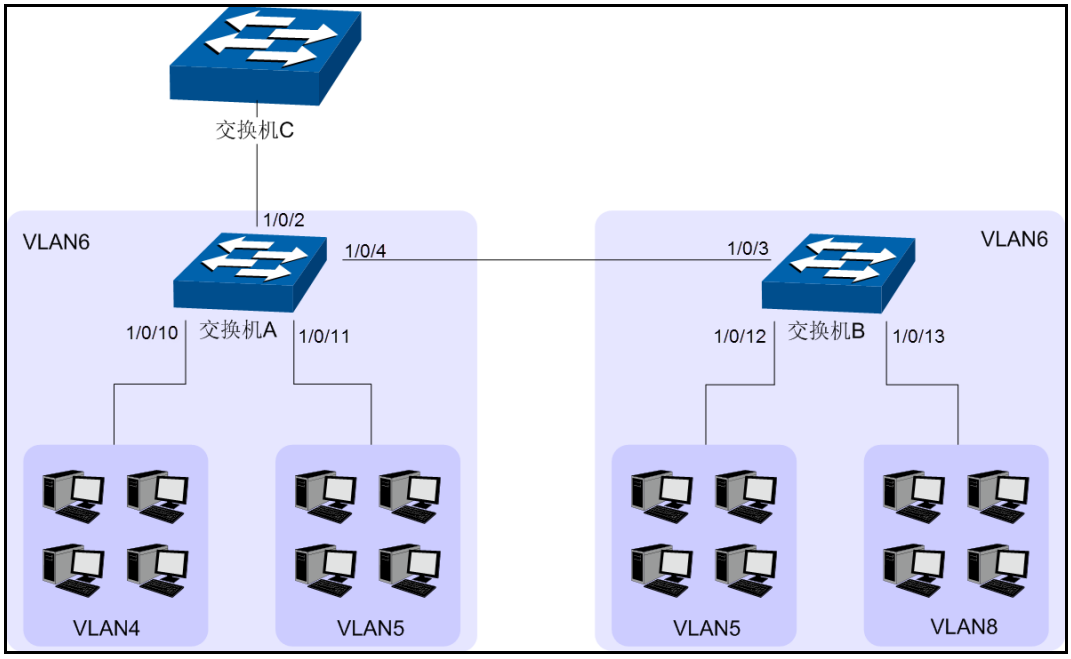
步骤	操作	说明
1	创建Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**功能页面创建Private VLAN。
2	配置成员端口	必选操作。在**VLAN>>Private VLAN>>端口配置**功能页面，设置端口属性并将端口添加到Private VLAN中。

7.9 Private VLAN功能的组网应用

➢ **组网需求**

- ISP向某公司提供了网络接入服务，连接到ISP机房的接入交换机A上，并通过VLAN6向企业提供网络服务；
- 企业中心交换机上连接了许多用户，各用户之间要求通过VLAN功能进行二层隔离；
- 中心交换机向下级联了另外一台汇聚层交换机，汇聚层交换机上配置了VLAN功能，部分VLAN要求和中心交换机上的VLAN进行连通，且所连接的用户均能够访问网络。

➢ **组网图**



➢ **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	创建Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**页面设置创建Private VLAN 6/4和Private VLAN 6/5。

步骤	操作	说明
2	为Private VLAN添加端口	必选操作。在**VLAN>>Private VLAN>>端口配置**页面，配置端口1/0/10的端口类型为Host并添加到Private VLAN 6/4中；配置端口1/0/11的端口类型为Host并添加到Private VLAN 6/5中；配置端口1/0/2和端口1/0/4的端口类型为Promiscuous并添加到Private VLAN 6/4中。

- 配置交换机B：

步骤	操作	说明
1	创建Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**页面设置创建Private VLAN 6/5和Private VLAN 6/8。
2	为Private VLAN添加端口	必选操作。在**VLAN>>Private VLAN>>端口配置**页面，配置端口1/0/12的端口类型为Host并添加到Private VLAN 6/5中；配置端口1/0/13的端口类型为Host并添加到Private VLAN 6/8中；配置端口1/0/3的端口类型为Promiscuous并添加到Private VLAN 6/5中。

回目录

第8章 生成树

STP（Spanning Tree Protocol，生成树协议）是根据IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

STP采用的协议报文是BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息，BPDU中包含了足够的信息来保证设备完成生成树的计算过程。STP即是通过在设备之间传递BPDU来确定网络的拓扑结构。

- **BPDU格式及字段说明**

要实现生成树的功能，交换机之间传递BPDU报文实现信息交互，所有支持STP协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。

标准生成树的BPDU帧格式及字段说明：

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Protocol identifier： 协议标识

Version： 协议版本

Message type： BPDU类型

Flag： 标志位

Root ID： 根桥ID，由两字节的优先级和6字节MAC地址构成

Root path cost： 根路径开销

Bridge ID： 桥ID，表示发送BPDU的桥的ID，由2字节优先级和6字节MAC地址构成

Port ID： 端口ID，标识发出BPDU的端口

Message age： BPDU生存时间

Maximum age： 当前BPDU的老化时间，即端口保存BPDU的最长时间

Hello time： 根桥发送BPDU的周期

Forward delay： 表示在拓扑改变后，交换机在发送数据包前维持在监听和学习状态的时间

- **STP的基本概念**

桥ID（Bridge Identifier）：桥ID是桥的优先级和其MAC地址的综合数值，其中桥优先级是一个可以设定的参数。桥ID越低，则桥的优先级越高，这样可以增加其成为根桥的可能性。

根桥（Root Bridge）：具有最小桥ID的交换机是根桥。请将环路中所有交换机当中最好的一台设置为根桥交换机，以保证能够提供最好的网络性能和可靠性。

指定桥（Designated Bridge）：在每个网段中，到根桥的路径开销最低的桥将成为指定桥，数据包将通过它转发到该网段。当所有的交换机具有相同的根路径开销时，具有最低的桥ID的交换机会被选为指定桥。

根路径开销（Root Path Cost）：一台交换机的根路径开销是根端口的路径开销与数据包经过的所有交换机的根路径开销之和。根桥的根路径开销是零。

桥优先级（Bridge Priority）：是一个用户可以设定的参数，数值范围从0到61440。设定的值越小，优先级越高。交换机的桥优先级越高，才越有可能成为根桥。

根端口（Root Port）：非根桥的交换机上离根桥最近的端口，负责与根桥进行通信，这个端口到根桥的路径开销最低。当多个端口具有相同的到根桥的路径开销时，具有最高端口优先级的端口会成为根端口。

指定端口（Designated Port）：指定桥上向本交换机转发数据的端口。

端口优先级（Port Priority）：数值范围从0到240，且必须是16的整数倍。端口优先级值越小，表示优先级越高，才越有可能成为根端口。

路径开销（Path Cost）：STP协议用于选择链路的参考值。STP协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

生成树基本概念的组网示意图如图 8-1所示。交换机A、B、C三者顺次相连，经STP计算过后，交换机A被选为根桥，端口2和端口6之间的线路被阻塞。

- 桥：交换机A为整个网络的根桥；交换机B是交换机C的指定桥。
- 端口：端口3和端口5分别为交换机B和交换机C的根端口；端口1和端口4分别为交换机A和交换机B的指定端口；端口6为交换机C的阻塞端口。

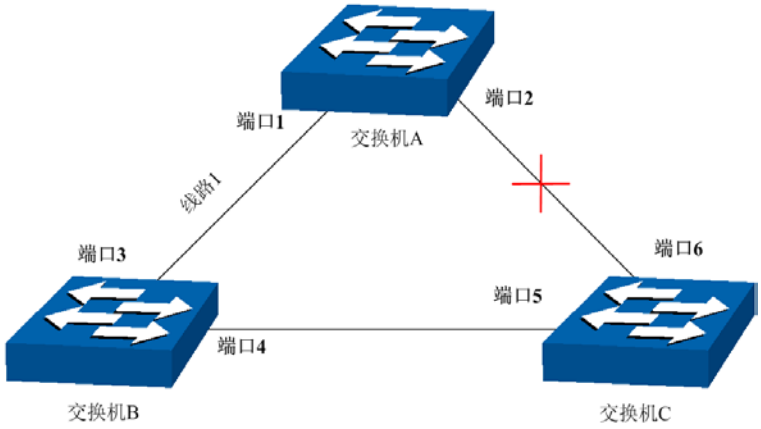


图 8-1 生成树基本概念组网图

➢ **STP定时器**

联络时间（Hello Time）：

数值范围从1秒到10秒。是指根桥向其它所有交换机发出BPDU数据包的时间间隔，用于交换机检测链路是否存在故障。

老化时间（Max. Age）：

数值范围从6秒到40秒。如果在超出老化时间之后，还没有收到根桥发出的BPDU数据包，那么交换机将向其它所有的交换机发出BPDU数据包，重新计算生成树。

传输时延（Forward Delay）：

数值范围从4秒到30秒。是指交换机的端口状态迁移所用的时间。

当网络故障引发生成树重新计算时，生成树的结构将发生相应的变化。但是重新计算得到的新配置消息无法立刻传遍整个网络，如果端口状态立刻迁移的话，可能会产生暂时性的环路。为此，生成树协议采用了一种状态迁移的机制，新的根端口和指定端口开始数据转发之前要经过2倍的传输时延，这个延时保证了新的配置消息已经传遍整个网络。

- **STP模式的BPDU的优先级比较原则**

假定有两条BPDU X和Y，则：

如果X的根桥ID小于Y的根桥 ID，则X优于Y；

如果X和Y的根桥ID相同，但X的根路径开销小于Y，则X优于Y；

如果X和Y的根桥ID和根路径开销相同，但X的桥ID小于Y，则X优于Y；

如果X和Y的根桥ID、根路径开销和桥ID相同，但X的端口ID小于Y，则X优于Y。

- **STP的计算过程**

- 初始状态

每台交换机在初始时会生成以自己为根桥的BPDU，根路径开销为0，指定桥ID为自身设备ID，指定端口为本端口。

- 最优BPDU的选择

每台交换机都向外发送自己的BPDU，同时也会收到其它交换机发送的BPDU。比较过程如下表所述：

步骤	内容
1	当端口收到的BPDU比本端口BPDU的优先级低时，交换机将丢弃接收到的BPDU，保留该端口的BPDU；否则，交换机将接收到的BPDU替换成为该端口的BPDU。
2	交换机将所有端口的BPDU进行比较，选出最优的BPDU作为本交换机的BPDU。

表 8-1 最优BPDU的选择

- 根桥的选择

通过交换配置消息，设备之间比较根桥ID，网络中根桥ID 最小的设备被选为根桥。

- 根端口、指定端口的选择

根端口、指定端口的选择过程如下表所述：

步骤	内容
1	非根桥交换机将接收到最优BPDU的那个端口指定为根端口。

步骤	内容
2	交换机根据根端口的BPDU和根端口的路径开销，为其它端口计算一个端口BPDU： • 根桥ID替换为根端口的根桥ID； • 根路径开销替换为根端口的根路径开销加上本端口到根端口的路径开销； • 指定桥ID替换为自身设备的ID； • 指定端口ID替换为自身端口ID。
3	交换机使用计算出来的BPDU和需要确定端口角色的端口上的BPDU进行比较，并根据比较结果进行不同的处理： • 如果计算出来的BPDU优，则设备就将该端口定为指定端口，端口上的BPDU被计算出来的BPDU替换，并周期性向外发送。 • 如果端口上的BPDU优，则设备不更新该端口BPDU并将此端口阻塞，该端口将不再转发数据，只接收但不发送配置消息；

表 8-2 根端口、指定端口的选择

说明：

- 在拓扑稳定状态，只有根端口和指定端口转发数据，其它的端口都处于阻塞状态，它们只接收BPDU报文而不转发数据。

➢ **RSTP**

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的STP，它大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。RSTP的端口状态实现快速迁移的前提如下：

- 根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。
- 指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

➢ **RSTP的基本概念**

边缘端口（Edge Port）：直接与终端相连而不是与其它交换机相连的端口。

点对点链路：是两台交换机之间直接连接的链路。

➢ **MSTP**

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在STP和RSTP的基础上，根据IEEE协会制定的802.1S标准建立的，它既可以快速收敛，也能使不同VLAN的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

MSTP的特点如下：

- MSTP通过VLAN-实例映射表，把VLAN和生成树联系起来，将多个VLAN捆绑到一个实例中，并以实例为基础实现负载均衡。
- MSTP把一个生成树网络划分成多个域，每个域内形成多棵内部生成树，各个生成树之间彼此独立。

- MSTP在数据转发过程中实现VLAN 数据的负载分担。
- MSTP 兼容STP 和RSTP。

➢ **MSTP的基本概念**

MST域（Multiple Spanning Tree Region，多生成树域）：由具有相同域配置和相同Vlan-实例映射关系的交换机所构成。

IST（Internal Spanning Tree，内部生成树）：MST域内的一棵生成树。

CST（Common Spanning Tree，公共生成树）：连接网络内所有MST域的单生成树。

CIST（Common and Internal Spanning Tree，公共和内部生成树）：连接网络内所有设备的单生成树，由IST和CST共同构成。

MSTP基本概念的组网图如图 8-2所示。

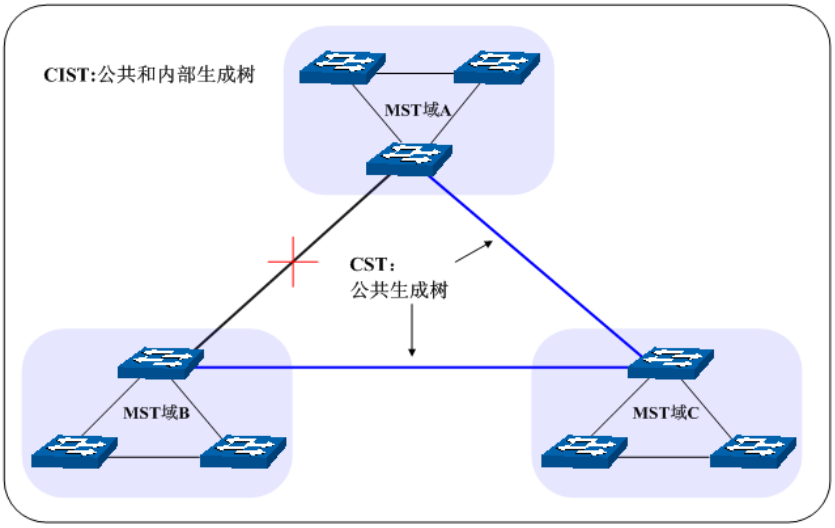


图 8-2 MSTP基本概念组网图

➢ **MSTP的基本原理**

MSTP将整个网络划分为多个MST域，各个域之间通过计算生成CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。MSTP同STP一样，使用BPDU进行生成树的计算，只是BPDU中携带的是MSTP的配置信息。

➢ **MSTP模式的BPDU优先级比较原则**

假定有两条MSTP的BPDU X和Y，则：

如果X的总根ID小于Y的总根ID，则X优于Y；

如果X和Y的总根ID相同，但X的外部路径开销小于Y，则X优于Y；

如果X和Y的总根ID和外部路径开销相同，但X的域根ID小于Y的域根ID，则X优于Y；

如果X和Y的总根ID、外部路径开销和域根ID相同，但X的内部路径开销小于Y，则X优于Y；

如果X和Y的总根ID、外部路径开销、域根ID和内部路径开销相同，但X的桥ID小于Y，则X优于Y；

如果X和Y的总根ID、外部路径开销、域根ID、内部路径开销和桥ID均相同，但X的端口ID小于Y，则X优于Y。

➢ **端口状态**

MSTP中，根据端口是否转发数据和如何处理BPDU报文，可将端口状态划分为以下四种：

- 转发：接收并转发数据，接收并发送BPDU报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送BPDU报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送BPDU报文，不进行地址学习。
- 断开：物理链路断开。

➢ **端口角色**

MSTP的端口角色分为以下几种：

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master端口：连接MST域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和Master端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口角色的示意图如图 8-3所示。

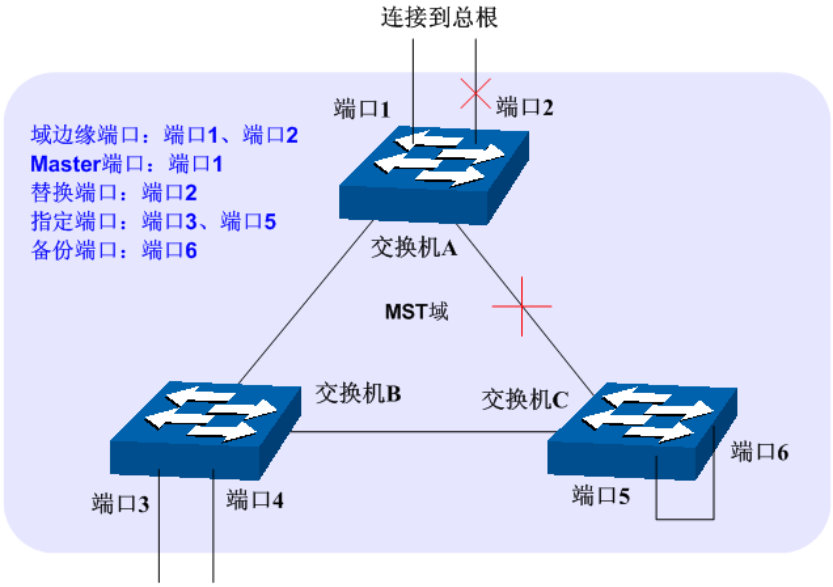


图 8-3 端口角色示意图

生成树模块主要用于配置交换机的生成树功能，包括**基本配置**、**端口配置**、**MSTP实例**以及**安全配置**四个部分。

8.1 基本配置

基本配置用于配置和查看交换机生成树功能的全局属性，本功能包括**基本配置**和**生成树信息**两个配置页面。

8.1.1 基本配置

配置生成树前您需要明确各交换机在每个生成树实例中所处的地位，每个生成树实例中只有一台交换机处于根桥地位。配置交换机的生成树功能，首先需要在本页配置交换机生成树的全局功能和相关参数。

进入页面的方法：生成树>>基本配置>>基本配置

图 8-4 基本配置

条目介绍：

- **全局配置**

  生成树功能： 选择是否启用交换机的生成树功能。

  生成树模式： 选择交换机的生成树模式。

  - STP：生成树兼容模式。
  - RSTP：快速生成树兼容模式。
  - MSTP：多重生成树模式。

- **参数配置**

  CIST优先级： 填写交换机的CIST优先级。CIST优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。值越小，表示优先级越高。默认为32768，且必须是4096的倍数。

  联络时间： 填写交换机发送协议报文的周期，用于检测链路是否存在故障。并且，2×(联络时间+1)≤老化时间。默认为2秒。

  老化时间： 填写协议报文在交换机中能够保存的最大生存期。默认为20秒。

  传输时延： 在网络拓扑改变后，交换机的端口状态迁移的延时时间。并且，2×(传输延时－1)≥老化时间。默认为15秒。

  流量限制： 填写在每个联络时间内，端口最多能够发送的协议报文的速度。默认为5pps。

  最大跳数： 填写协议报文被转发的最大跳数，限制生成树的规模，默认20跳。

注意：

- 设备的传输时延参数的长短与STP的规模有关。如果传输时延过小，可能会引入临时的环路；如果传输时延过大，网络可能会较长时间不能恢复连通，建议采用默认值。
- 合适的联络时间可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果联络时间过长，在链路发生丢包时，交换机会误以为链路出现了故障，从而引发网络中生成树的重新计算；如果联络时间过短，交换机将频繁发送重复的配置消息，增加了交换机的负担，浪费了网络资源，建议采用默认值。
- 如果老化时间过小，交换机会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果老化时间过大，交换机不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力，建议采用默认值。
- 如果流量限制过大，每个联络时间内发送的MSTP报文数会很多，从而占用过多的网络资源，建议采用默认值。

8.1.2 生成树信息

本页用来查看交换机生成树功能的相关参数。

进入页面的方法：生成树>>基本配置>>生成树信息

生成树信息

开启状态：	启用
STP版本：	MSTP
本桥：	32768---00-02-03-c0-9a-d3
总根：	32768---00-02-03-c0-9a-d3
外部路径开销：	0
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:43:30
拓扑改变次数：	1

MSTP实例信息

实例ID：	1
开启状态：	启用
本桥：	32768---00-02-03-c0-9a-d3
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:44:41
拓扑改变次数：	1

刷新

图 8-5 基本信息

8.2 端口配置

本页用来配置交换机端口的CIST参数。

进入页面的方法：生成树>>端口配置

图 8-6 端口配置

条目介绍：

- **端口配置**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选端口配置端口STP功能，可多选。

端口： 显示交换机的端口号。

状态： 选择该端口是否启用STP功能。

优先级： 确定与该端口连接的端口是否会被选为根端口的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。默认为128，范围0-240，且为16的倍数。

外部路径开销： 在不同MST域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

内部路径开销： 在MST域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

边缘端口： 选择是否启用边缘端口。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

点对点链路： 选择端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

协议迁移： 启用端口开始一次协议迁移检查。

端口工作模式： 显示端口所处的生成树模式。

端口角色： 显示端口在生成树实例中担任的角色。

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master端口：连接多生成树域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和Master端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口状态： 显示端口所处的工作状态。

- 转发：接收并转发数据，接收并发送协议报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送协议报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送协议报文，不进行地址学习。
- 断开：物理链路断开。

LAG： 显示端口当前所属的汇聚组。

注意：

- 对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动BPDU保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。
- 对于属于汇聚组的端口，所有端口都可以被配置成与点对点链路相连。
- 当端口被设置为与点对点链路相连，则该端口所在的所有生成树实例均被设置为与点对点链路相连。如果端口实际物理链路不是点对点链路，而您配置为强制点对点链路，则有可能会引入临时环路。

8.3 MSTP实例

MSTP设置了VLAN-实例映射表（即VLAN和生成树的对应关系表），把VLAN和生成树联系起来。通过增加MSTP实例（将多个VLAN整合到一个集合中），将多个VLAN捆绑到一个实例中，并以实例为基础实现负载均衡。

只有当多台交换机的MST域名、MST域的修订级别、VLAN-实例映射表完全相同时，它们才能属于同一个MST域。本功能包括**域配置**、**实例配置**和**实例端口**三个配置页面。

8.3.1 域配置

本页用来配置MST域的域名和修订级别。

进入页面的方法：生成树>>MSTP实例>>域配置

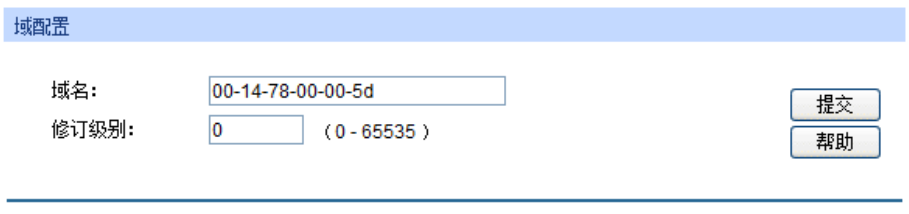


图 8-7 域配置

条目介绍：

- **域配置**

  域名： 填写域名来标识MST域，最长可用32个字符。

  修订级别： 填写修订级别来标识MST域。

8.3.2 实例配置

实例配置是MST域的一个属性，用来描述VLAN和生成树实例的映射关系。您可以按需要将VLAN分配至不同的实例，每个实例就是一个“VLAN组”，不受其它实例和公共生成树的影响。

进入页面的方法：生成树>>MSTP实例>>实例配置

图 8-8 实例配置

条目介绍：

- **VLAN-实例映射**

  实例ID： 填写实例ID。

  VLAN ID： 填写需要添加的VLAN ID。若对应实例ID中已有VLAN ID，在此修改后，新的VLAN ID将被添加，而不会将之前的覆盖。

- **实例配置**

  选择： 勾选条目配置实例状态及优先级，可多选。

  实例ID： 显示交换机的实例ID号。

  状态： 显示相应实例的状态。

  优先级： 在对应实例ID中，确定该交换机是否会被选为根桥的重要依据。默认为32768，且必须是4096的倍数。

  VLAN ID： 填写该实例ID所包含的VLAN ID。若之前已存在VLAN ID，在此修改后，之前的VLAN ID将被清空，并映射至CIST中。

注意：

- 当GVRP和MSTP同时启用时，GVRP报文将沿着生成树实例CIST进行传播。因此如果希望通过GVRP在网络中发布某个VLAN，则需在配置MSTP的“VLAN-实例映射”时保证把这个VLAN映射到CIST上。关于GVRP的相关介绍请参见GVRP。

8.3.3 实例端口

端口在不同的生成树实例中可以担任不同的角色，本页用来配置不同实例ID中的端口的参数，同时在此可以查看端口在特定实例中的状态信息。

进入页面的方法：生成树>>MSTP实例>>实例端口

图 8-9 实例端口

条目介绍：

- **实例端口配置**

实例ID：	选择需要配置端口属性的实例ID。
UNIT：	根据UNIT ID选择指定的交换机进行配置。
选择：	勾选端口配置端口的优先级和路径开销，可多选。
端口：	显示交换机的端口号。
优先级：	在对应实例中，确定与该端口连接的端口是否会被选为根端口的重要依据。默认为128，范围0-240，且为16的倍数。
路径开销：	在MST域内的对应实例中，用于选择路径和计算路径开销的参考值，并作为该端口被选为根端口的依据。值越小，表示优先级越高。

端口角色： 显示端口在生成树实例中担任的角色。

端口状态： 显示端口所处的工作状态。

LAG： 显示端口当前所属的汇聚组。

注意：

- 同一端口在不同的生成树实例中的端口状态可以不同。

生成树功能全局配置步骤：

步骤	操作	说明
1	明确交换机在生成树实例中的角色：根桥或指定桥	准备工作。
2	配置MSTP的全局参数	必选操作。在**生成树>>基本配置>>基本配置**页面，开启交换机的生成树功能，并配置MSTP的参数。
3	配置端口的MSTP参数	必选操作。**生成树>>端口配置>>端口配置**页面进行配置。
4	配置MST域	必选操作。**生成树>>MSTP实例>>域配置**、**实例配置**页面，创建MST域，及交换机在MST域中的角色。
5	配置实例端口的MSTP参数	可选操作。**生成树>>MSTP实例>>实例端口**页面，为MST域内不同的实例，配置实例端口的MSTP属性。

8.4 安全配置

通过配置设备的保护功能，来防止生成树网络中的设备遭受各种形式的恶意攻击。本功能包括**端口保护**和**TC保护**两个配置页面。

8.4.1 端口保护

- **环路保护：**

在网络拓扑稳定时，交换机通过不断接收上游交换机发送的BPDU报文，来保持本机各个端口的端口状态。但是当发生链路拥塞或者单向链路故障时，位于下游的交换机无法收到BPDU报文，将会重新计算生成树，重新选择端口角色，这时阻塞端口会迁移到转发状态，从而导致网络中产生环路。

环路保护功能会抑制这种环路的产生。对于启用了环路保护的端口，当没有接收到上游交换机发送的BPDU报文，引起STP重新计算时，不论其端口角色如何，该端口将一直被设置为阻塞状态。

- **根桥保护：**

在设计网络拓扑时，CIST的根桥和备份根桥大多处于一个高带宽的核心域内。但是，当维护人员错误配置或遭受到网络中的恶意攻击时，网络中的合法根桥有可能会收到优先级更高的BPDU报文，致使当前合法根桥失去了根桥的地位，从而导致网络拓扑结构的错误变动。这种错误的变动，使得原来应该通过高速链路的流量被牵引到低速链路上，引起网络拥塞。

为了防止这种情况发生，MSTP提供根桥保护功能：对于启用了根桥保护功能的端口，它在所有实例上的端口角色只能为“指定端口”。当该端口收到优先级更高的BPDU时，立刻将该端口的端口状态转化为“阻塞”状态，不再转发报文（相当于将此端口相连的链路断开）。当在2倍的传输时延时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

- **TC保护**

交换机收到TC-BPDU报文（网络拓扑发生变化的通知报文）后，会将本机的地址表项删除。当有人伪造TC-BPDU报文恶意攻击交换机时，交换机短时间内收到大量TC-BPDU报文，频繁的删除操作给交换机带来很大负担，给网络的稳定带来很大隐患。通过在交换机上启用TC保护功能，可以避免交换机频繁地删除地址表项。

启用TC保护功能后，交换机在“TC保护周期”内，收到TC-BPDU的最大数目为“TC保护阈值”处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

- **BPDU保护**

交换机上直接与PC或服务器相连的端口会被设置为“边缘端口”，以实现这些端口的快速迁移。当这些端口接收到BPDU报文时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。而这些端口一般情况下不会收到BPDU报文。如果有人用伪造的BPDU报文恶意攻击交换机，就会引起网络拓扑的震荡。

MSTP提供BPDU保护功能来防止这种攻击：启用了BPDU保护功能后，如果边缘端口收到了BPDU报文，MSTP就将这些端口关闭，同时通知网管这些端口被MSTP关闭，被关闭的端口只能由网络管理人员来恢复。

- **BPDU过滤**

BPDU过滤用来防止恶意的BPDU洪泛攻击。交换机收到恶意的BPDU报文以后，会向网络中的其它交换机转发，致使网络内的交换机不停的进行STP计算，从而导致交换机的CPU占用率过高或者BPDU报文的协议状态错误等。

启用了BPDU报文过滤功能的端口，将不再接收和转发任何BPDU报文，但是会向外发送自身的BPDU报文，从而防止交换机受到BPDU报文的攻击，保证STP计算的正确性。

在本页可以对交换机的各个端口配置上述几种保护功能，建议您对符合条件的端口启用相应的保护功能。

进入页面的方法：生成树>>安全配置>>端口保护

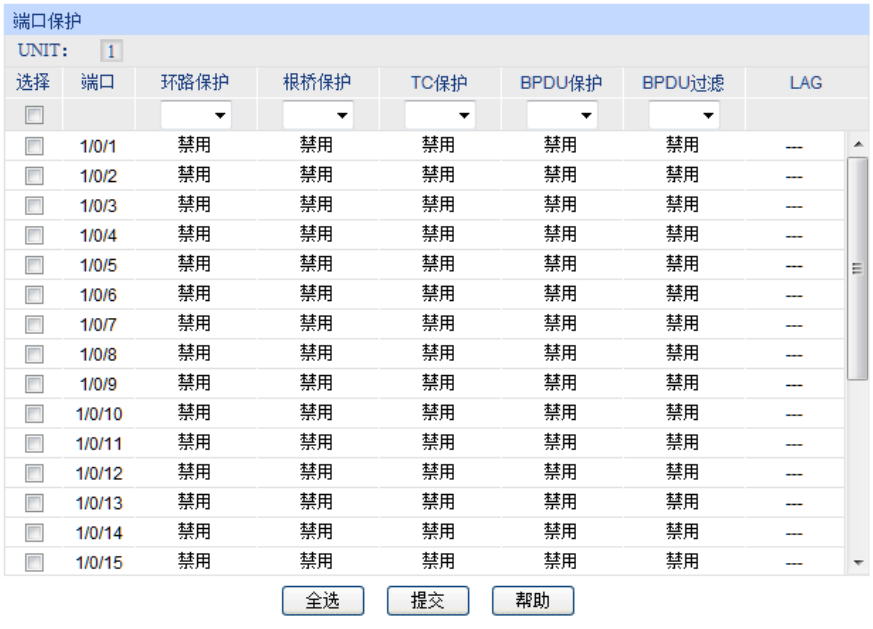


图 8-10 端口保护

条目介绍：

- **端口保护**

UNIT：	根据UNIT ID选择指定的交换机进行配置。
选择：	勾选端口配置端口保护功能，可多选。
端口：	显示交换机的端口号。
环路保护：	防止由于链路拥塞或者单向链路故障，导致下游设备重新计算生成树，由此产生的网络环路现象。
根桥保护：	防止当前合法根桥失去根桥的地位而引起网络拓扑结构的错误变动。
TC保护：	防止由于恶意伪造的TC报文在STP协议网络中传播而导致桥设备的地址表不断清空所引起的网络吞吐量下降。
BPDU保护：	防止边缘端口受到恶意伪造的协议报文的攻击。
BPDU过滤：	防止STP协议网络中协议报文泛洪。
LAG：	显示端口当前所属的汇聚组。

8.4.2 TC保护

当**端口保护**页面开启端口的“TC保护”功能后，需要在本页对TC保护的TC保护阈值和TC保护周期进行配置。

进入页面的方法：生成树>>安全配置>>TC保护

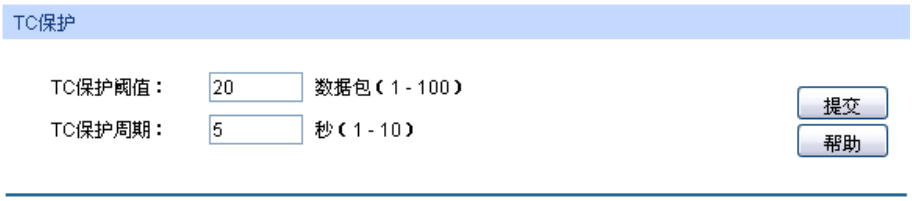


图 8-11 TC保护

条目介绍：

- **TC保护**

TC保护阈值：	在TC保护周期内，交换机收到TC报文的最大数目。超过该数目后，交换机在该周期内不再进行地址表删除操作。默认为20数据包。
TC保护周期：	填写TC保护的周期。默认为5秒。

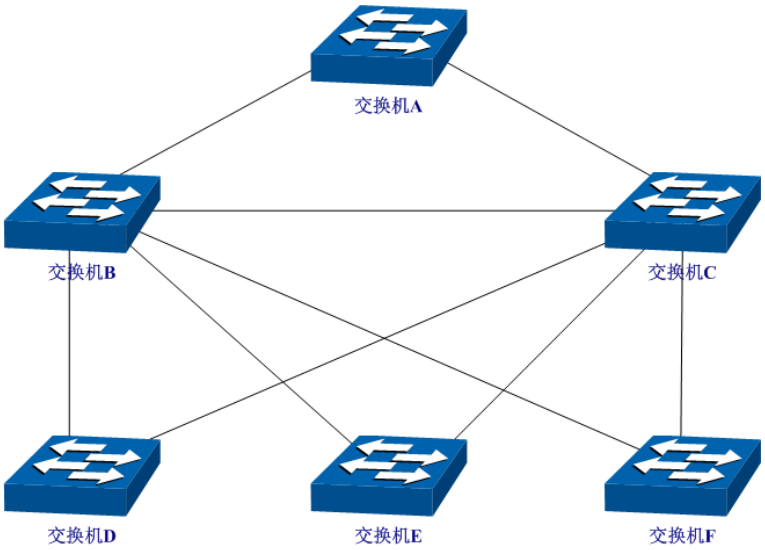
8.5 STP功能的组网应用

- **组网需求**

- 交换机A、B、C、D、E均支持MSTP功能；
- A为中心交换机；

- B、C为汇聚层交换机，D、E、F为接入层交换机；
- 整个网络中共有6个VLAN，为VLAN101-VLAN106；
- 所有设备运行MSTP，并且所有设备均属于同一个MST域；
- VLAN101、103和105的数据流量以B为根桥，VLAN102、104和106的数据流量以C为根桥。阻断网络中的环路，并能达到数据转发过程中VLAN数据的冗余备份以及负载分担效果。

➢ **组网图**



➢ **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见7.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择MSTP生成树模式。 在**生成树>>端口配置>>端口配置**页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在**生成树>>MSTP实例>>域配置**页面，配置域名为“**TP-LINK**”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在**生成树>>MSTP实例>>实例配置**页面，配置VLAN-实例映像表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。

- 配置交换机B：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见7.1 802.1Q VLAN。

步骤	操作	说明
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择MSTP生成树模式。 在**生成树>>端口配置>>端口配置**页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在**生成树>>MSTP实例>>域配置**页面，配置域名为“**TP-LINK**”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在**生成树>>MSTP实例>>实例配置**页面，配置VLAN-实例映像表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。
5	将交换机B配置为实例1的根桥	在**生成树>>MSTP实例>>实例配置**页面，将实例1的优先级设置为0
6	将交换机B配置为实例2的指定桥	在**生成树>>MSTP实例>>实例配置**页面，将实例2优先级设置为4096

- 配置交换机C

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见7.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择MSTP生成树模式。 在**生成树>>端口配置>>端口配置**页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在**生成树>>MSTP实例>>域配置**页面，配置域名为“**TP-LINK**”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在**生成树>>MSTP实例>>实例配置**页面，配置VLAN-实例映像表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。
5	将交换机C配置为实例1的指定桥	在**生成树>>MSTP实例>>实例配置**页面，将实例1的优先级设置为4096。
6	将交换机C配置为实例2的根桥	在**生成树>>MSTP实例>>实例配置**页面，将实例2优先级设置为0。

- 配置交换机D

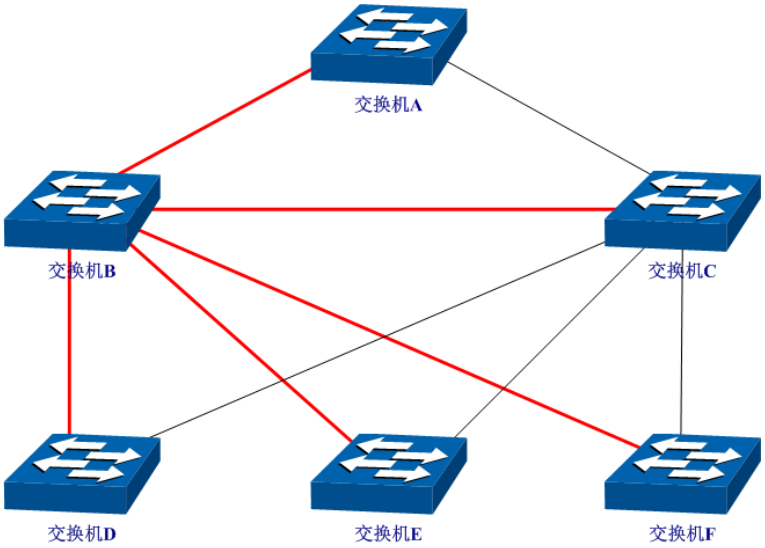
步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见7.1 802.1Q VLAN。

步骤	操作	说明
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择MSTP生成树模式。 在**生成树>>端口配置>>端口配置**页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在**生成树>>MSTP实例>>域配置**页面，配置域名为“**TP-LINK**”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在**生成树>>MSTP实例>>实例配置**页面，配置VLAN-实例映像表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。

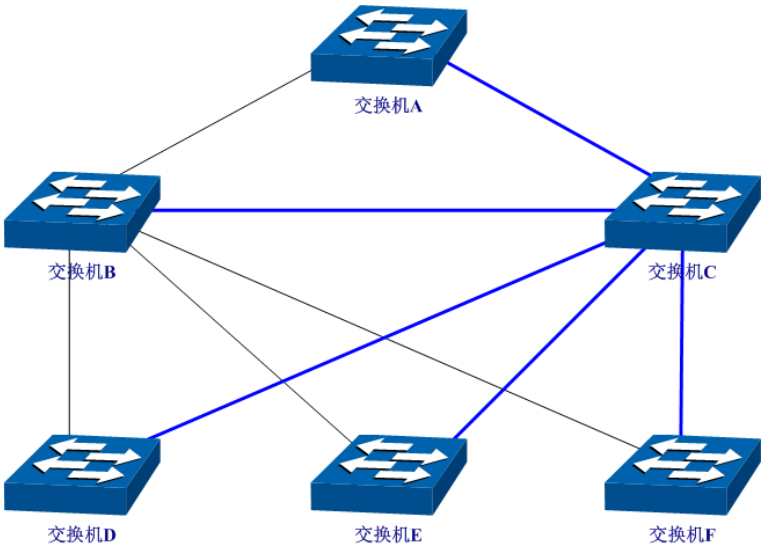
- 交换机E和交换机F的配置方法同交换机D

➢ **拓扑稳定以后两个实例所生成的动态拓扑结构**

- 对于实例1（VLAN 101 103 105）而言，连通的链路为下图中红色的路径，灰色的路径断开。



- 对于实例2（VLAN 102 104 106）而言，连通的链路为下图中蓝色的路径，灰色的路径断开。



➢ **配置建议**

- 所有交换机的端口均建议启用“TC保护”功能。
- 根桥交换机的所有端口建议启用“根桥保护”功能。
- 非边缘端口建议启用“环路保护”功能。
- 连接PC与服务器的边缘端口，建议启用“BPDU保护”或“BPDU过滤”功能。

回目录

第9章 组播管理

➢ 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。数据采用单播（Unicast）方式传输时，服务器会为每一个接收者单独传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，这样将会大量占用网络资源。数据采用广播（Broadcast）方式传输时，系统会把信息一次性的传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（Multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如图 9-1所示。

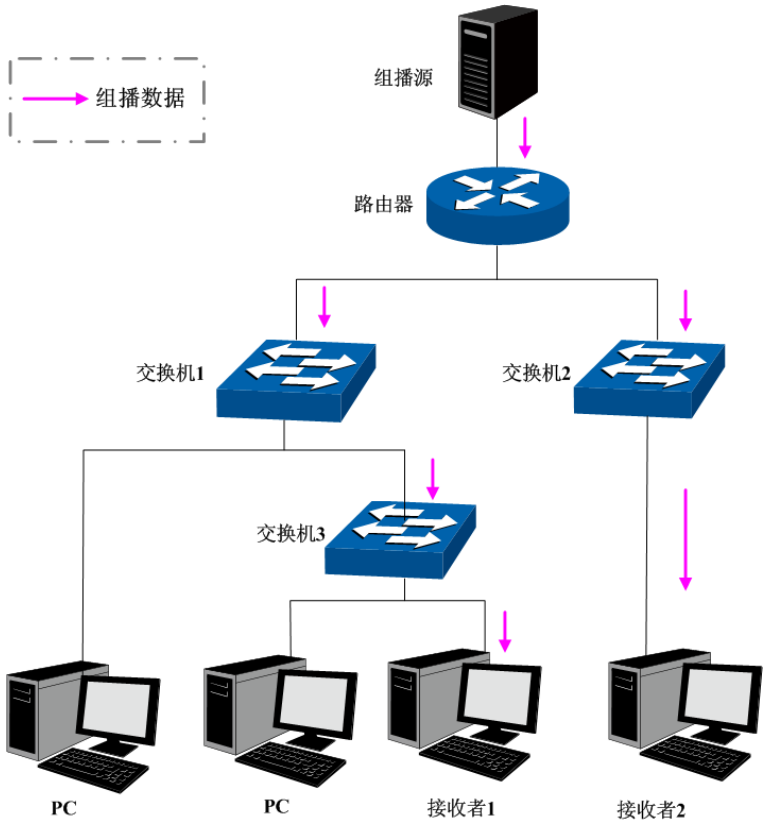


图 9-1 组播传输信息的方式

组播的特点是：

- 服务对象不固定，通常是一对多的关系；
- 把服务对象看成一个组，发送端只需要发送一次数据到相关网络设备即可；
- 每个用户可以随时加入或退出组播组；
- 实时性要求较高，允许一定的丢帧现象发生。

- **组播地址**

组播IP地址：

根据IANA（Internet Assigned Numbers Authority，因特网编号授权委员会）规定，组播报文的IP地址使用D类IP地址，组播IP地址范围是224.0.0.0～239.255.255.255。其中，几个特殊组播IP地址段的范围及说明如下：

组播地址范围	说明
224.0.0.0～224.0.0.255	路由协议及其它底层拓扑发现和维护协议的保留地址
224.0.1.0～224.0.1.255	会议及电视会议
239.0.0.0～239.255.255.255	局域网内部使用地址，不能用于Internet

表 9-1 特殊的组播IP地址段

组播MAC地址：

以太网传输单播IP报文的时候，目的MAC地址使用的是接收者的MAC地址。但是在传输组播报文时，传输目标不再是一个具体的接收者，而是一个成员不确定的组，所以需要使用组播MAC地址作为目的地址，组播MAC地址是一个逻辑的MAC地址。

IANA规定，组播MAC地址的高24bit位是以01-00-5E开头，低23bit为组播IP地址的低23bit，映射关系如图 9-2所示：

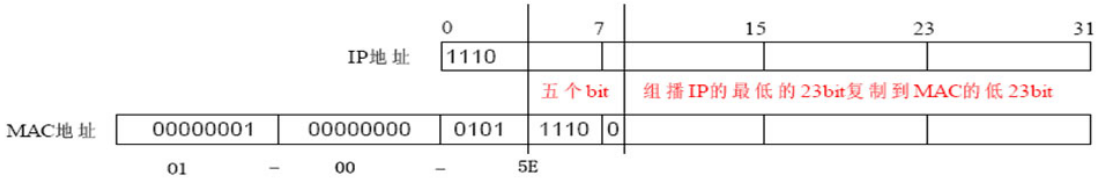


图 9-2 组播MAC地址和组播IP地址的对应关系

由于IP组播地址的高4bit是1110，标识了组播组，而低28bit中只有23bit被映像到组播MAC地址上，这样IP组播地址中就会有5bit没有使用，从而出现了32个IP组播地址映像到同一MAC地址上的结果。

- **组播地址表**

交换机在转发组播数据时是根据组播地址表来进行的。由于组播数据不能跨越VLAN传输，因此组播地址表的第一部分是VLAN ID，当交换机收到组播数据包时，数据包只能在接收端口所在的VLAN内转发。组播地址表对应的出口端口不是一个，而是一组端口列表。转发数据时，交换机根据组播数据的目的组播地址查找组播地址表，如果在组播地址表中查不到相应的条目，则把该组播数据广播，即向接收端口所在VLAN内的所有端口上转发；如果能查找到对应的条目，则目的地址应该是一组端口列表，于是交换机把这个组播数据复制成多份，每份转发到一个端口，从而完成组播数据的交换。组播地址表一般格式如图 9-3所示。

VLAN ID	组播IP	端口

图 9-3 组播地址表

- **IGMP侦听**

网络中的主机通过发送IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP侦听（IGMP Snooping）是组播约束机制，交换机用他来完成组播组的

动态注册，运行IGMP侦听的交换机通过侦听和分析主机与组播路由器之间交互的IGMP报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

组播管理模块主要用于配置交换机的组播管理功能，包括**IGMP侦听**、**组播地址表**、**组播过滤**以及**报文统计**四个部分。

9.1 IGMP侦听

- **IGMP侦听的工作过程**

交换机侦听用户主机与路由器之间的交互IGMP报文，跟踪组播信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（IGMP Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（IGMP Leave）时，路由器会发送该端口的特定组查询报文（Group-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（IGMP Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

- **IGMP报文**

运行了IGMP侦听的交换机对不同类型的IGMP报文的处理方法如下。

1. 查询报文（IGMP Query）。

由路由器发出，又可分为通用查询报文和特定组查询报文。路由器定时发出通用查询报文，以查询该网段有哪些组播组的成员。当路由器收到IGMP离开报文后，会通过接收端口向该组播组发送IGMP特定组查询报文，交换机会将此报文转发，以确定该端口中是否还有组播组的其它组成员。

对于通用查询报文，交换机会将此报文通过VLAN内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

对于特定组查询报文，交换机要向被查询的组播组的成员转发IGMP特定组查询报文。

2. 报告报文（IGMP Report）。

由主机发出，当主机想主动加入某一组播组或对路由器查询报文给予响应时产生此种报文。

在收到IGMP报告报文时，交换机将此报文通过VLAN内的路由器端口转发出去，同时从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

3. 离开报文（IGMP Leave）。

运行IGMPv1的主机离开组播组时不会发送IGMP离开报文，因此交换机无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送IGMP 报告报文，因此当其对应的成员端口时间超时后，交换机就会将该端口从相应的组播地址表中删除。运行IGMPv2或IGMPv3的主机离开组播组时，会通过发送IGMP离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到IGMP离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组查询报文，然后重置成员端口时间为离开滞后时间，离开滞后时间超时后，交换机将此端口从相应的组播地址表中删除。如果删除离开端口后组播组中没有其它组成员存在，则将整个组播组删除。

➢ **IGMP侦听的基本概念**

1. 相关端口

路由器端口（Router Port）：交换机上连接路由组播设备的端口。

成员端口（Member Port）：交换机上连接组播组成员的端口。

2. 相关定时器

路由器端口时间：这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是300秒。

成员端口时间：这段时间内，如果交换机没从成员端口接收到报告报文，就认为该成员端口不再有主机属于多播组。默认是260秒。

离开滞后时间：从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。默认是1秒。

本功能包括**基本配置**、**端口参数**、**VLAN参数**、**组播VLAN**和**查询器配置**五个配置页面。

9.1.1 基本配置

配置本交换机的IGMP侦听功能，首先要在本页配置IGMP侦听的全局功能和相关参数。

如果交换机收到的组播数据没有在组播地址表内，该组播数据会在VLAN内广播；当交换机启用“未知组播报文丢弃”功能后，交换机收到不在组播地址表中的组播数据报文时，会将此报文丢弃，从而节省带宽，并提高系统的处理效率，请根据实际情况配置该功能。

进入页面的方法：组播管理>>IGMP侦听>>基本配置

图 9-4 基本配置

条目介绍：

➢ **全局配置**

IGMP侦听：	选择是否启用交换机的IGMP侦听功能。
未知组播报文：	选择交换机对未知组播报文的处理方法。

➢ **IGMP侦听信息**

描述：	显示IGMP侦听的配置项。
成员：	显示对应配置项的成员。

9.1.2 端口参数

本页用来配置交换机端口的IGMP侦听属性。

进入页面的方法：组播管理>>IGMP侦听>>端口参数

图 9-5 端口参数

条目介绍：

- **端口配置**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选条目配置端口的IGMP侦听功能，可多选。

端口号： 显示交换机的端口号。

IGMP侦听： 选择该端口是否启用IGMP侦听功能。

快速离开功能： 当端口启动快速离开功能后，交换机收到IGMP离开报文时，直接将该端口从组播组中删除。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口的快速离开功能只能在主机支持IGMPv2或v3时生效。
- 当快速离开功能与“未知组播报文丢弃”功能同时开启的情况下，如果某个端口下有多个用户，一个用户的快速离开，可能会造成同一组播组中其它用户的组播业务中断。

9.1.3 VLAN参数

IGMP侦听所建立的组播组是基于VLAN广播域的，不同的VLAN可以设置不同的IGMP参数。本页用于配置每个VLAN的IGMP侦听参数。

进入页面的方法：组播管理>>IGMP侦听>>VLAN参数

图 9-6 VLAN参数

条目介绍：

- **VLAN参数**

VLAN ID：	填写启用IGMP侦听功能的VLAN ID。
路由器端口时间：	在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐300秒。
成员端口时间：	在所设时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口失效。推荐260秒。
离开滞后时间：	主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐1秒。
静态路由器端口：	点选路由器端口，静态路由器端口多用于拓扑稳定的网络中。

- **VLAN列表**

选择：	勾选条目配置VLAN参数，可多选。
VLAN ID：	显示VLAN ID。
路由器端口时间：	显示VLAN的路由器端口时间。
成员端口时间：	显示VLAN的成员端口时间。
离开滞后时间：	显示VLAN的离开滞后时间。
静态路由器端口：	显示VLAN的静态路由器端口。
动态路由端口：	显示VLAN的动态路由器端口。
操作：	点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<提交>按键，使修改内容生效。

注意：

- 当“组播VLAN”功能启用时，本页的配置将失效。

配置步骤：

步骤	操作	说明
1	启用IGMP侦听功能	必选操作。在**组播管理>>IGMP侦听>>基本配置**、**端口参数**页面，启用交换机的IGMP侦听功能和端口的IGMP侦听功能。
2	配置VLAN的组播参数	可选操作。在**组播管理>>IGMP侦听>>VLAN参数**页面，为交换机的各个VLAN配置组播参数。 没有配置组播参数的VLAN，表示没有在该VLAN内开启IGMP侦听功能，那么该VLAN中的组播数据会广播。

9.1.4 组播VLAN

对于传统的组播数据转发方式，当处于不同VLAN的用户加入同一个组播组时，组播路由器会为每个包含接收者的VLAN复制并转发一份组播数据。这样的组播点播方式，浪费了大量的带宽。

通过配置组播VLAN，可以有效的解决上述问题。将交换机的端口加入到组播VLAN中，使不同VLAN内的用户共享一个组播VLAN接收组播数据，组播数据只在组播VLAN内进行传输，从而节省了带宽。同时由于组播VLAN与普通的VLAN完全隔离，安全和带宽都得以保证。

配置组播VLAN之前，需要在**802.1Q VLAN**功能处预先配置一个VLAN作为组播VLAN，并将相应的端口加入此VLAN中。组播VLAN启用后，在**VLAN参数**页面中为其它VLAN配置的组播参数将失效，即组播数据不再通过除组播VLAN以外的其它VLAN转发。

进入页面的方法：组播管理>>IGMP侦听>>组播VLAN

图 9-7 组播VLAN

条目介绍：

- **组播VLAN**

  组播VLAN： 选择是否启用组播VLAN。

VLAN ID： 填写组播VLAN的VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐300秒。

成员端口时间： 在所设时间内，如果交换机没从成员端口接收到报告报文，就认为该成员端口失效。推荐260秒。

离开滞后时间： 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐1秒。

动态路由器端口： 显示目前加入组播VLAN的动态路由器端口。

静态路由器端口： 点选端口区配置静态路由器端口，静态路由器端口，多用于拓扑稳定的网络中。

注意：

- 路由器端口必须均在组播VLAN中，否则成员端口无法收到组播数据。
- 必须在**802.1Q VLAN**功能处完成端口的相关VLAN属性配置，组播VLAN才能正常运行。
- 组播VLAN中的成员端口的端口类型推荐为GENERAL。
- 组播VLAN中的路由器端口的端口类型必须配置为TRUNK或者是出口规则为“带tag”的GENERAL端口，否则组播VLAN内的所有的组播成员端口都无法接收到组播数据。
- 建立了组播VLAN后，所有的IGMP报文只在组播VLAN内处理。

配置步骤：

步骤	操作	说明
1	启用IGMP侦听功能	必选操作。在**组播管理>>IGMP侦听>>基本配置**、**端口参数**页面，启用交换机的IGMP侦听功能和端口的IGMP侦听功能。
2	创建组播VLAN	必选操作。在**VLAN>>802.1Q VLAN**功能处，创建组播VLAN，并将所有成员端口和路由器端口加入该VLAN中。 ● 配置成员端口的端口类型为GENERAL。 ● 配置路由端口的端口类型为TRUNK或出口规则为“带tag”的GENERAL。
3	配置组播VLAN的参数	可选操作。进入**组播管理>>IGMP侦听>>组播VLAN**页面，启用组播VLAN并配置组播VLAN的组播参数。时间参数建议使用默认值。
4	查看配置情况	若配置成功，则在**组播管理>>IGMP侦听>>基本配置**页面中的“已启用的VLAN”条目处，显示组播VLAN的VLAN ID。

9.1.5 查询器配置

在运行了IGMP的组播网络中，需要一台三层组播设备充当IGMP查询器，负责发送IGMP查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。而网络中的二层设备可以通过侦听三层组播设备与主机之间交互的IGMP报文来建立二层组播转发表项，实现二层组播转发。但是，在一个没有三层组播设备的网络中，由于没有设备负责IGMP查询器的功能，

这样网络中不会周期性存在IGMP协议交互的报文，二层设备也无法通过侦听IGMP报文来建立二层的组播转发表项。为了解决这个问题，可以在二层设备上使用IGMP侦听查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。本页面主要用于配置IGMP侦听查询器的相关参数。

进入页面的方法：组播管理>>IGMP侦听>>查询器配置

图 9-8 组播VLAN

条目介绍：

- **IGMP侦听查询器配置**

VLAN ID：	输入需要启动查询器特性的VLAN ID。
查询间隔：	输入查询间隔时间。查询器会按照间隔时间发送通用查询报文。
最大响应时间：	输入查询报文的最大响应时间字段的值。
通用查询报文源IP：	输入通用查询报文源IP地址。
最后监听成员查询间隔：	输入最后监听成员查询间隔时间。交换机收到成员端口的离开报文后，将会按照查询间隔发送特定组查询报文检查是否还有其他组播成员。
最后监听成员查询次数：	输入最后监听成员查询次数。交换机收到成员端口的离开报文后，将会发送该次数的特定组查询报文检查是否还有其他组播成员。
特定组查询报文源IP：	输入特定组查询报文源IP地址。

- **IGMP侦听查询器列表**

查看IGMP侦听查询器的详细配置参数。

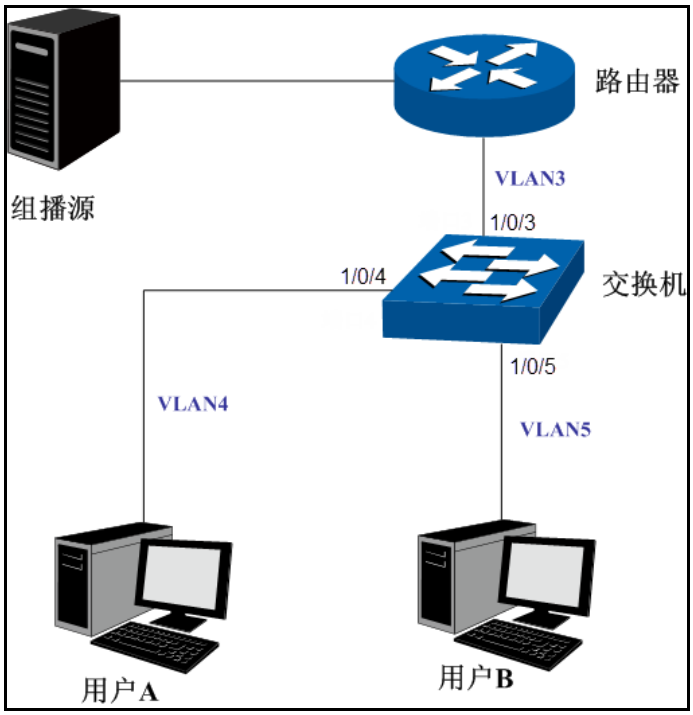
9.2 IGMP侦听功能组网应用

- **组网需求**

- 组播源通过路由器转发组播数据，组播数据流通过交换机被转发到接收端用户A和用户B。
- 路由器：WAN口与组播源相连；LAN口与交换机相连，且通过VLAN3转发数据。
- 交换机：端口1/0/3与路由器相连，且通过VLAN3转发数据；端口1/0/4与用户A相连，且通过VLAN4转发数据；端口1/0/5与用户B相连，且通过VLAN5转发数据。

- 用户A：与交换机的端口1/0/4相连。
- 用户B：与交换机的端口1/0/5相连。
- 配置组播VLAN，使用户A和用户B通过组播VLAN接收组播数据。

➢ **组网图**



➢ **配置步骤**

配置交换机：

步骤	操作	说明
1	创建VLAN	在**VLAN>>802.1Q VLAN**功能处，创建VLAN3、4、5，并将VLAN3的描述填写为“组播VLAN”。
2	配置端口属性	在**VLAN>>802.1Q VLAN**功能处。 配置端口1/0/3的端口类型为GENERAL，出口规则TAG，并加入VLAN3、4、5中。 配置端口1/0/4的端口类型为GENERAL，出口规则UNTAG，并加入VLAN3、4中。 配置端口1/0/5的端口类型为GENERAL，出口规则UNTAG，并加入VLAN3、5中。
3	启用IGMP侦听	在**组播管理>>IGMP侦听>>基本配置**页面，启用IGMP侦听功能。 在**组播管理>>IGMP侦听>>端口配置**页面，启用端口1/0/3、1/0/4、1/0/5的IGMP侦听功能。
4	启用组播VLAN	在**组播管理>>IGMP侦听>>组播VLAN**页面，启用组播VLAN，并配置组播VLAN的VLAN ID为3，其它参数建议使用默认值。
5	检查组播VLAN	在**组播管理>>IGMP侦听>>基本配置**页面，“IGMP侦听信息”处，“已启用的端口”显示为1/0/3、1/0/4、1/0/5，“已启用的VLAN”显示为3。

9.3 组播地址表

在网络中，信息接收者可以加入各自所需的组播组，交换机在转发组播数据时是根据组播地址表来进行的。本功能包括**地址表显示**和**静态地址表**两个配置页面。

9.3.1 地址表显示

在本页可以查看到交换机中已存在的所有组播地址表信息。

进入页面的方法：组播管理>>组播地址表>>地址表显示

图 9-9 地址表显示

条目介绍：

- **显示设置**

可以直接查看所有的组播地址表，也可以根据组播IP、VLAN ID、转发端口查询特定的组播地址表信息。

- **组播IP表**

组播IP： 显示组播IP地址。

VLAN ID： 显示组播组对应的VLAN ID。

转发端口： 显示组播组的转发端口。

地址类型： 显示组播IP的地址类型。

注意：

- 若改变**VLAN参数**或**组播VLAN**页面中的参数，交换机组播地址表中的动态组播地址表项会受到影响。

9.3.2 静态地址表

静态组播地址表不是通过IGMP侦听学习到的，不受动态组播组及组播过滤的影响，对于某些固定的组播组，可以提高数据传输质量并增加安全性。

进入页面的方法：组播管理>>组播地址表>>静态地址表

图 9-10 静态地址表

条目介绍：

- **新建条目**

组播IP： 填写静态绑定的组播IP地址。

VLAN ID： 填写组播IP对应的VLAN ID。

转发端口： 点选端口设置为组播IP的转发端口。

- **显示设置**

显示设置： 选择静态组播IP表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：显示全部静态组播IP表条目。
- 组播IP：设置欲查找条目需包含的组播IP地址信息。
- VLAN ID：设置欲查找条目需包含的VLAN ID信息。
- 转发端口：设置欲查找条目需包含的端口。

- **静态组播表**

选择： 勾选条目进行删除，可多选。

组播IP： 显示绑定的组播IP地址。

VLAN ID： 显示组播组对应的VLAN ID。

转发端口： 显示组播组的转发端口。

9.4 组播过滤

在启用了IGMP侦听后，可以通过配置组播过滤，来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。

当用户申请加入某个组播组时，会发送IGMP报告报文，该报文到达交换机后，交换机首先检查接收端口上所配置的组播过滤规则，如果此端口可以加入这个组播组，则将这个端口加入到该组播组的地址表中；否则交换机就丢弃该IGMP报告报文，这样组播数据就不会转发到该端口，从而控制了用户加入组播组。

9.4.1 Profile配置

本界面主要配置需要过滤的组播地址段。

进入页面的方法：组播管理>>组播过滤>>Profile配置

图 9-11 创建Profile

条目介绍：

- **创建IGMP Profile**

  Profile ID： 输入Profile ID，区间为1-999。

  模式： 配置该Profile的过滤模式。
  - 允许：只有组播地址属于过滤地址范围时，才处理组播报文。
  - 拒绝：只处理组播地址不在过滤地址范围内的组播报文。

- **显示设置**

  显示设置： 选择IGMP Profile信息的显示规则，可以帮助您快速查找到所需的条目。
  - 全部：显示全部IGMP Profile信息。
  - Profile ID：输入欲查找条目需包含的Profile ID。

- **IGMP Profile信息**

  选择： 勾选后可以删除Profile条目。

  Profile ID： 显示Profile ID。

模式： 显示Profile的过滤模式。

绑定端口： 显示当前绑定了该Profile的端口。

操作： 点击<编辑>按键为Profile添加具体的过滤组播地址，如下图所示。

图 9-12 创建Profile

条目介绍：

- **Profile模式**

  Profile ID： 显示Profile ID。

  模式： 修改该Profile的过滤模式，需提交才能生效。

- **添加IP范围**

  起始地址： 显示过滤地址段的起始组播IP地址。

  结束地址： 显示过滤地址段的结束组播IP地址。

- **IP范围**

  选择： 勾选后可以删除IP地址段条目。

  序号： 显示IP地址段的序列号。

  起始地址： 显示IP地址段的起始组播IP地址。

  结束地址： 显示IP地址段的结束组播IP地址。

9.4.2 Profile绑定

本页用来配置端口与Profile进行绑定，使组播过滤功能生效。

进入页面的方法：组播管理>>组播过滤>>Profile绑定

图 9-13 Profile绑定

条目介绍：

- **Profile与最大加入组数目绑定**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选条目配置端口的组播过滤功能，可多选。

端口： 显示交换机的端口号。

Profile ID： 配置端口绑定的Profile组播过滤文件。

最大加入组数目： 配置端口可以加入到最大组播组数目。

溢出操作： 当端口所加入组播组数已达到最大组播组数时，如果要加入更多的组播组，交换机将执行的动作。

- 丢弃：不再加入新的组播组。
- 替换：端口加入新的组播组，并将端口从当前已加入的组播组IP地址最小的组播组中移除。

LAG： 显示端口当前所属的汇聚组。

清除绑定： 清除端口绑定的Profile。

注意：

- 组播过滤功能只对启用了IGMP侦听的VLAN生效。
- 组播过滤功能对静态组播IP不生效。
- 一个端口只能绑定一个Profile。

配置步骤：

步骤	操作	说明
1	配置Profile	必选操作。在**组播管理>>组播过滤>>Profile配置**页面，创建Profile并设置组播过滤地址。
2	配置端口的组播过滤规则	必选操作。在**组播管理>>组播过滤>>Profile绑定**页面，配置端口与Profile绑定。

9.5 报文统计

在本页可以查看交换机各端口的组播报文流量信息，便于监控网络中IGMP报文。

进入页面的方法：组播管理>>报文统计

图 9-14 报文统计

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为5秒。

- **IGMP报文统计**

UNIT： 根据UNIT ID选择查看指定交换机侦听到的IGMP报文。

端口： 显示交换机的端口号。

查询报文数： 显示端口接收到的查询报文的数目。

报告报文(V1)： 显示端口接收到的IGMPv1报告报文的数目。

报告报文(V2)： 显示端口接收到的IGMPv2报告报文的数目。

报告报文(V3)： 显示端口接收到的IGMPv3报告报文的数目。

离开报文： 显示端口接收到的离开报文的数目。

错误报文： 显示端口接收到的错误报文的数目。

回目录

第10章 路由功能

说明：

本章节提及的路由器是指传统意义上的路由器或者运行了路由协议的以太网交换机。

在网络中通常由传统路由器或者运行了路由协议的以太网交换机实现不同网络间的数据转发。路由是指路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径上的最后一个路由节点则将数据转发给目标主机。

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。常用的路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。路由表中的每一个路由条目基本都包含如下基本属性：

- 目的网络地址：用于标识该条路由条目所指向的目标网络。
- 子网掩码：用于标识目标网络的子网掩码。
- 下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。
- 下一跳接口：用于标识数据从本地发出的出接口。

路由条目的来源有三种，分别为直连路由、静态路由和动态路由。

1) 直连路由：通过数据链路层协议发现的，通常为与路由器直接连接的网络的路由。
2) 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。
3) 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。

本交换机的路由模块主要支持直连路由和静态路由两种，直连路由即为本地直连网络的路由，如本地配置的 VLAN 进行工作组划分时，同时提供代理 ARP 功能来满足特定网络需求，功能模块主要包括五个部分。

10.1 接口

网络接口是一种三层模式下的虚拟接口，主要用于实现 VLAN、路由端口之间的三层互通。每个 VLAN 接口对应一个 VLAN，路由端口对应一个物理端口，环回接口是纯软件接口的。网络接口通过地址与子网掩码参数确定了一个 IP 网段（或称为 IP 子网），并作为该网段的网关对需要跨网段的报文进行基于 IP 地址的三层转发。

进入界面的方法：路由功能>>接口>>接口设置

图 10-1 接口设置

条目介绍：

- **创建接口**

接口 ID： 选择需要配置 IP 地址的接口 ID，如 VLAN ID、交换机端口号、环回接口。

IP 地址模式： 设置 IP 地址申请模式。

- None：无 IP。
- Static：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

IP 地址： 设置网络接口的 IP 地址。

子网掩码： 设置网络接口 IP 地址的子网掩码。

管理状态： 设置网络接口的管理状态，默认为使能。选择“禁用”来关闭此接口的三层功能。

接口名称： 设置网络接口的接口名称。

- **接口列表**

选择： 选择接口条目进行修改或删除。

ID： 显示该网络接口对应的 ID。

模式： 显示 IP 地址申请模式。

IP 地址： 显示网络接口的 IP 地址。

子网掩码： 显示该网络接口的子网掩码。

接口名称： 显示该网络接口的接口名称。

状态： 显示网络接口的当前运行状态。

操作： 单击“编辑”修改网络接口设置， 或单击“详细”查看详细信息。

点击“编辑”来修改选定接口条目的参数：

图 10-2 修改接口

- **修改接口**

ID： 显示接口 ID。

IP 地址模式： 设置 IP 地址申请模式。

- None：无 IP。
- Static：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

IP 地址： 设置接口的 IP 地址。

子网掩码： 设置接口的子网掩码。

管理状态： 修改接口的管理状态。

接口名： 修改接口名称。

点击“详细”来查看接口的详细配置信息：

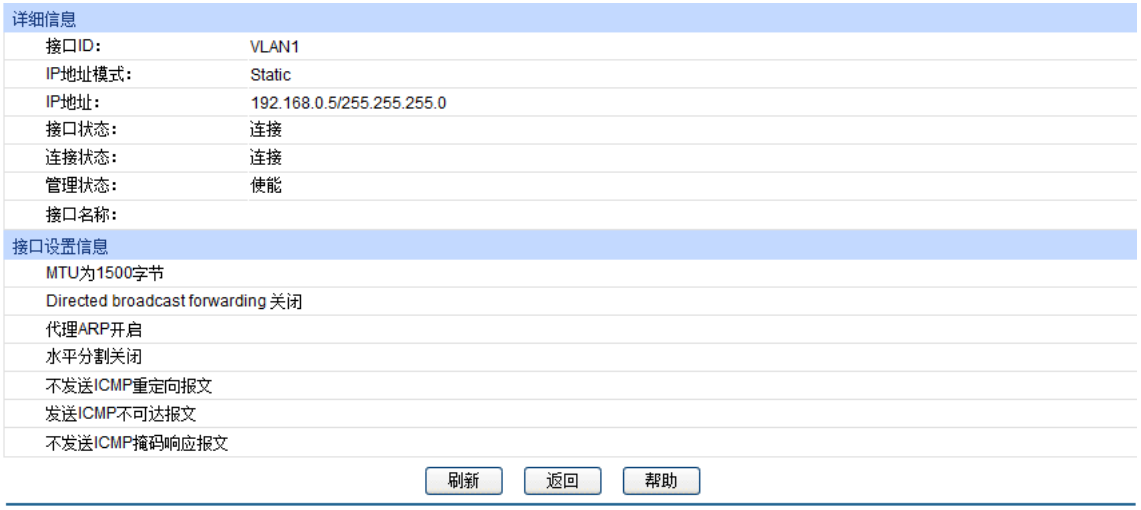


图 10-3 接口详细信息

- **详细信息**

接口 ID： 显示接口 ID。

IP 地址模式： 显示 IP 地址申请模式。

- None：无 IP。
- Static：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

接口状态： 显示网络接口当前状态。只有设置了 IP，管理状态为“开启”，并且连接状态为“连接”时，接口状态才为“连接”。

连接状态： 显示是否有已连接端口接入到当前网络接口。

管理状态： 显示网络接口管理状态。如果显示为“关闭”， 那么接口的三层功能将被关闭。

接口名： 修改接口名称。

- **接口设置信息**

  显示接口的 MTU，代理 ARP 功能，ICMP 报文等相关信息。

10.2 路由表

此页面用来显示交换机上保存的路由条目，来源包括：直连路由，静态路由和动态路由协议。

进入界面的方法：路由功能>>路由表>>路由表

图 10-4 路由表

条目介绍：

- **路由信息汇总**

路由协议： 本条路由条目的来源：

- static：静态路由。
- connected：直连路由。
- RIP：RIP 路由协议。
- OSPF：OSPF 路由协议。

目的网络： 目的网络 IP 地址及子网掩码。

下一跳地址： 下一跳 IP 地址。

管理距离： 管理距离。

接口名称： 接口名称。

10.3 静态路由

静态路由是由网络管理员手动设置的路由，在组网结构比较简单的网络中，网络管理员只需手工配置静态路由即可实现网络互通。静态路由一般在规模不大、拓扑结构固定的网络中配置。在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。当网络发生改变时则需要网络管理员再次修改配置参数以保证网络正常通信。

10.3.1 静态路由条目

本页面用于添加静态路由条目。管理员可以在该静态路由条目页面配置一条缺省路由来防止路由表过大。当路由表中不存在与 IP 报文的目的 IP 地址匹配表项时，就选择缺省路由转发。

进入界面的方法：路由功能>静态路由>>静态路由条目

图 10-5 静态路由条目

条目介绍：

- **静态路由条目添加**

  目的地址： 设置路由条目需要到达的目标网络地址。

  子网掩码： 设置路由条目需要到达的目标网络的子网掩码。

  下一跳地址： 设置通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 指定路由条目的管理距离。管理距离越小，优先级越高。

- **静态路由条目**

  选择： 选择静态路由条目进行修改或删除。

  目的地址： 显示路由条目需要到达的目标网络地址。

  子网掩码： 显示路由条目需要到达的目标网络的子网掩码。

  下一跳地址： 修改通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 修改路由条目的管理距离。管理距离越小，优先级越高。

  度量值： 显示路由条目的度量值。

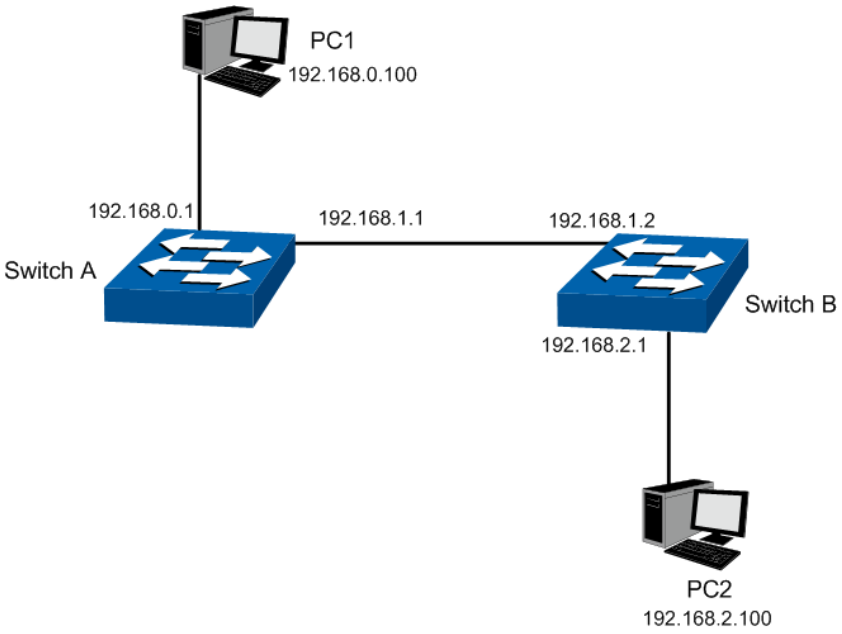
  静态路由条目数： 显示表中的静态路由条目数量。

10.3.2 静态路由功能的组网应用

➢ **组网需求**

1. 某小型企业网络中有三个 VLAN，分别为 VLAN10、20、30，VLAN ID 分别为 10、20、30。
2. PC1 在 VLAN10，PC2 在 VLAN30；PC1 和 PC2 可以网络互通。

➢ **组网图**



➢ **配置步骤**

● **配置交换机 A**

步骤	操作	说明
1	添加接口 10	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 10，IP 地址模式为 static，IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，接口名称为 VLAN10。
2	添加接口 20	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 20，IP 地址模式为 static，IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，接口名称为 VLAN20。
3	添加静态路由条目	在**路由功能>>静态路由>>静态路由条目**页面添加一条静态路由条目，目的地址为 192.168.2.0，子网掩码为 255.255.255.0，下一跳为 192.168.1.2。

● **配置交换机 B**

步骤	操作	说明
1	添加接口 20	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 20，IP 地址模式为 static，IP 地址为 192.168.1.2，子网掩码为 255.255.255.0，接口名称为 VLAN20。

步骤	操作	说明
2	添加接口 30	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 30，IP 地址模式为 static，IP 地址为 192.168.2.1，子网掩码为 255.255.255.0，接口名称为 VLAN30。
3	添加静态路由条目	在**路由功能>>静态路由>>静态路由条目**页面添加一条静态路由条目，目的地址为 192.168.0.0，子网掩码为 255.255.255.0，下一跳为 192.168.1.1。

- **配置所有 PC**

设置 PC1 默认网关为 192.168.0.1；配置 PC2 的默认网关为 192.168.2.1。

10.4 DHCP 服务器

➢ **DHCP 服务器的应用环境**

DHCP 服务器可以在下列场景中高效完成网络设备的 IP 地址配置工作：

1) 网络规模大，为每台网络设备手工配置网络参数的工作量较大，且不便于对网络进行集中管理。

2) 网络中设备数目大于该网络支持的设备数量，相应的 IP 资源不足。例如，ISP 限制同时接入网络的用户数目，而网络中的设备并不需要同时访问网络，则用户可以动态按需获得网络 IP。

3) 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

➢ **DHCP 服务器在 T3700G-28TQ 上的实现**

下图为我司交换机 T3700G-28TQ 配置为 DHCP 服务器时的网络拓扑图示范，具体的网络环境可能根据实际需求有所调整。

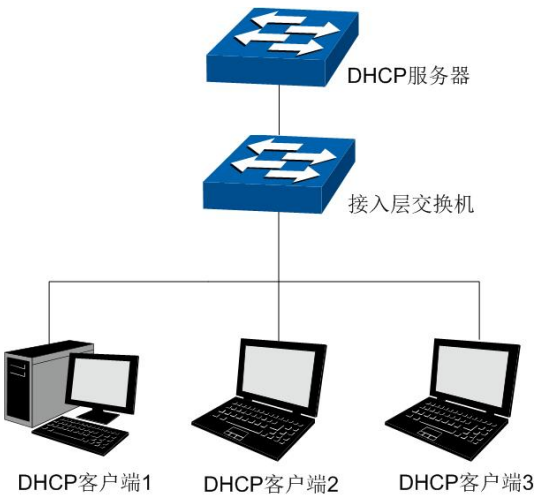


图 10-6 DHCP 服务器拓扑图示例

为了使网络中的设备能够安全顺利的获得 IP 地址，保证网络的稳定性，T3700G-28TQ 交换机的 DHCP 服务器功能可以完成如下所示任务：

- T3700G-28TQ 为网络中的多个 VLAN 指定特定的地址池，实现不同 VLAN 的设备获得不同网段的 IP 地址。
- 当客户端向 T3700G-28TQ 申请 IP 地址时，T3700G-28TQ 判断接收请求报文的端口所属的默认 VLAN，从该 VLAN 接口 IP 所属的地址池中选取合适的地址分配给客户端。

- 如果服务器和客户端之间搭建了 DHCP 中继设备，DHCP 请求报文经过 DHCP 中继设备时报文中的 giaddr 字段将被填入中继设备上客户端连接的接口 IP 地址，服务器将在此 IP 网段地址池中选择合适的 IP 地址分配给客户端。如果 DHCP 服务器上没有创建中继设备 IP 地址段的地址池，客户端将无法获得 IP 地址。
- IP 地址重复分配检测功能，避免因同一地址重复分配而造成的网络中 IP 冲突。

➢ **IP 地址重复分配检测**

当 T3700G-28TQ 交换机配置了 DHCP 服务器功能为网络中的设备分配 IP 地址时，为防止 IP 地址重复分配导致 IP 地址冲突，交换机将对该地址进行 Ping 探测。地址检测方式如下：

DHCP 服务器发送目的 IP 地址为待分配地址的 ICMP 回显请求报文，如果在等待时间内收到响应报文，DHCP 服务器从地址池中选择新的 IP 地址，并重复上述探测操作；如果在指定时间内没有收到回显响应报文，则将地址分配给客户端，从而确保客户端被分得的 IP 地址唯一。

➢ **分配 IP 地址的优先次序**

T3700G-28TQ 交换机的 DHCP 服务器功能为客户端分配 IP 地址时，其分配规则如下：

1) DHCP 服务器中与客户端 MAC 地址手动绑定的 IP 地址。
2) DHCP 服务器曾经分配给客户端的 IP 地址。
3) 客户端发送的 DHCP-DISCOVER 报文中指定的 IP 地址。
4) 选择合适的地址池，从中顺序查找可供分配的第一个 IP 地址。

➢ **DHCP 服务器在 T3700G-28TQ 上的配置要点**

1) 为每个网段保留特定的 IP 地址不做分配，如网关地址、网段广播地址、服务器地址等。
2) 为特殊用户群手动绑定静态 IP，当收到特殊用户群的 IP 申请时，交换机将为客户端分配租期为无限长的固定的 IP 地址。
3) 创建动态分配地址池，网络中的设备申请 IP 地址时，可以获得相应接口地址池中的空闲地址。

DHCP 服务器功能包括 **DHCP 服务器**、**地址池设置**、**静态绑定**，**绑定表和报文统计五**个配置页面。

10.4.1 DHCP 服务器

在这个页面中，请使能 DHCP 服务器功能，同时设置某些预留地址不做分配，如特定用户群、服务器地址等特殊地址均可以设置为保留地址不做分配。

进入页面的方法：**路由功能>>DHCP 服务器>>DHCP 服务器**

图 10-7 DHCP 服务器

条目介绍：

- **全局配置**

  DHCP 服务器： 选择是否启用 DHCP 服务器功能。

- **Ping 设置**

设置用于确定 IP 是否已存在的 Ping 报文的个数以及超时时间。

Ping 报文数： 每次确定 IP 存在的时候发出的报文数。

Ping 超时： Ping 超过该时间则认为指定 IP 不存在。

- **不分配 IP 设置**

起始 IP 地址： 显示预留 IP 地址段的起始地址。

结束 IP 地址： 显示预留 IP 地址段的结束地址。

- **不分配 IP 列表**

选择： 选择以删除指定的预留 IP 地址段。

序号: IP 地址段的序列号。

起始 IP 地址： 显示预留 IP 地址段的起始地址。

结束 IP 地址： 显示预留 IP 地址段的结束地址。

10.4.2 地址池设置

在这个页面中，请为不同的网段分别配置 DHCP 地址池，包含默认网关、DNS 域名服务器和租期等参数。

进入页面的方法：**路由功能>>DHCP 服务器>>地址池设置**

图 10-8 DHCP 服务器地址池

条目介绍：

- **DHCP 服务器地址池**

地址池名称：	填写地址池的名称，以便于区分各个地址池的实际属性。
网络号：	配置此地址池的网络地址，同一网段中的地址除了预留地址以及特殊地址外均可以作为可分配地址。
掩码：	配置此地址池的子网掩码。当客户端从此地址池获取 IP 地址时，其子网掩码以此参数为准。
租期：	配置此地址池中分配的 IP 地址租期。默认为 120 分钟。
默认网关：	展开右边的输入框在下方的输入框中配置此地址池的默认网关，最大可设置 8 个，为可选配置。默认情况下，也可以以 VLAN 接口 IP 地址作为默认网关。
DNS 服务器：	展开右边的输入框在下方的输入框中配置此地址池的 DNS 服务器，最大可设置 8 个，为可选配置。默认情况下，也可以以 VLAN 接口 IP 地址作为 DNS 服务器。

- **地址池列表**

选择：	勾选地址池条目进行删除，可多选。
名称：	显示地址池名称。
网络号：	显示地址池的网络地址。
掩码：	显示地址池的子网掩码。
租期：	显示地址池的租期。
操作：	点击编辑或查看按钮来对条目进行编辑或查看。

10.4.3 静态绑定

在这个页面中，可以将可将 MAC 地址与 IP 地址进行绑定，服务器收到已绑定 MAC 的 DHCP 请求时，会将所绑定的 IP 地址发送给客户端。

进入页面的方法：**路由功能>>DHCP 服务器>>静态绑定**

图 10-9 静态绑定

条目介绍：

- **DHCP 服务器静态绑定设置**

地址池名称：	地址池的名称，从已配置地址池中选取。
绑定 IP：	与 MAC 地址绑定的 IP 地址。
绑定方式：	设定 IP 与客户端 ID 绑定或者 IP 与硬件地址绑定。
客户端 ID：	绑定的客户端 ID。
硬件地址：	所绑定的 MAC 地址。
硬件类型：	选择为 Ethernet 或者 IEEE802 类型。

- **静态绑定列表**

选择：	勾选静态绑定条目进行删除，可多选。
地址池名称：	显示地址池的名称。
客户端 ID：	显示绑定的客户端 ID。
硬件地址：	显示所绑定的 MAC 地址。
IP 地址：	显示与 MAC 地址绑定的 IP 地址。
硬件类型：	显示硬件类型。
操作：	点击<编辑>按钮来对选定条目进行编辑。

10.4.4 绑定表

在此页面中，可以查看从交换机成功获得 IP 地址的租约信息。

进入页面的方法：**路由功能>>DHCP 服务器>>绑定表**

图 10-10 绑定表

条目介绍：

- **已分配 IP 列表**

选择： 勾选绑定条目进行删除。

ID： 显示绑定条目的 ID。

IP 地址： 显示客户端获得的 IP 地址。

客户端 ID/MAC 地址： 显示客户端的 ID/MAC 地址。

类型： 显示该绑定条目的类型。

剩余租期： 显示客户端获得的 IP 地址的剩余生效时间。

10.4.5 报文统计

本页面用来查看交换机接收或发送的 DHCP 报文数目。

进入页面的方法：**路由功能>>DHCP 服务器>>报文统计**

图 10-11 DHCP 报文统计

条目介绍：

- **接收报文**

BOOTREQUEST： 显示接收到的 Bootp Request 报文数目。

DHCPDISCOVER： 显示接收到的 Discover 报文数目。

DHCPREQUEST： 显示接收到的 Request 报文数目。

DHCPDECLINE： 显示接收到的 Decline 报文数目。

DHCPRELEASE： 显示接收到的 Release 报文数目。

DHCPINFORM： 显示接收到的 Inform 报文数目。

➢ **发送报文**

BOOTREPLY： 显示发送的 Bootp Reply 报文数目。

DHCPOFFER： 显示发送的 Offer 报文数目。

DHCPACK： 显示发送的 ACK 报文数目。

DHCPNAK： 显示发送的 NAK 报文数目。

DHCP 服务器配置步骤（VLAN 接口为例）：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	创建 VLAN 接口	必须操作。在**路由功能>>接口>>接口设置**页面中为 VLAN 建立 VLAN 接口。
4	启用 DHCP 服务器功能	必须操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中启用 DHCP 服务器功能。
5	配置预留 IP 地址	可选操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中配置预留 IP 地址不做分配。
6	配置 IP 地址池	必须操作。在**路由功能>>DHCP 服务器>>地址池设置**页面中配置 IP 地址池参数，包括子网掩码、默认网关、DNS 和租期等。
7	手动绑定 IP 地址	可选操作。在**路由功能>>DHCP 服务器>>静态绑定**页面中可以为特殊客户端绑定特定的 IP 地址。

10.4.6 DHCP 服务器功能的组网应用

➢ **网络需求**

- 将校园中每一栋楼划分独立的 VLAN，并属于不同的 IP 网段；
- 每一栋楼中的接入点分成两部分，一部分是办公室，配有固定计算机，采用静态 IP 地址；另一部分是教室，多为笔记本电脑接入，采用动态 IP 地址，需要从网络中的 DHCP 服务器上获取 IP 地址；
- DNS 服务器位于 VLAN 1 中，IP 为 160.20.30.2。

➢ **组网图**

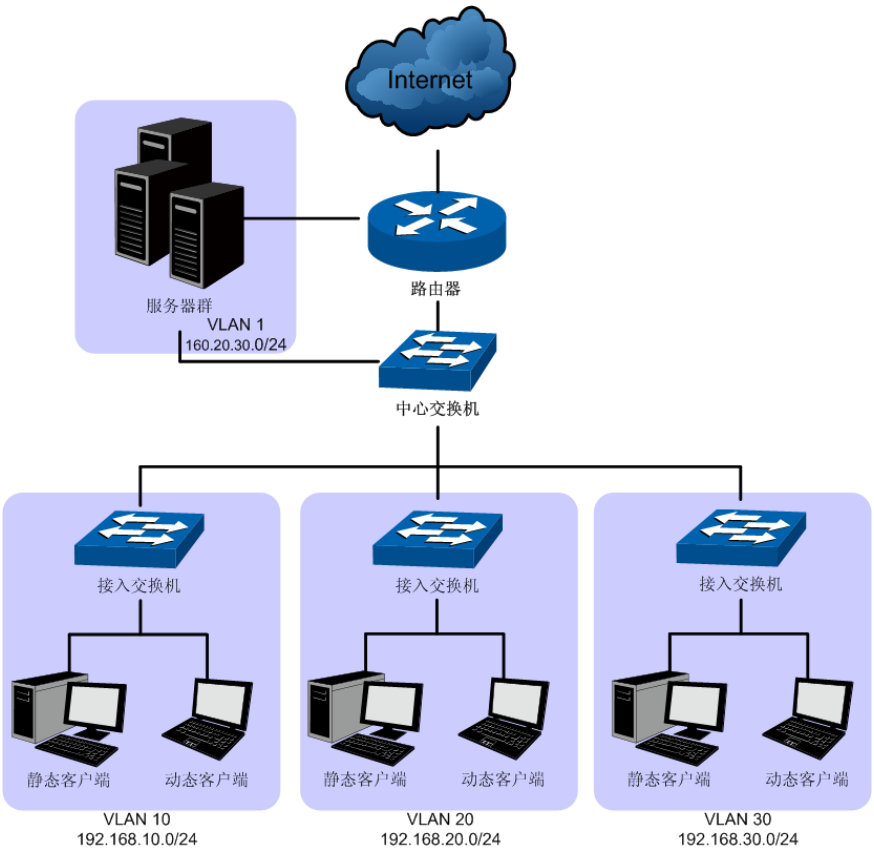


图 10-12 DHCP 服务器功能组网图

中心交换机采用 T3700G-28TQ，并启用 DHCP 服务器为网络中的设备分配 IP 地址，配置步骤如下：

➢ **配置步骤**

配置中心交换机：

步骤	操作	说明
1	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN10, VLAN20 和 VLAN30，并配置端口。
2	创建 VLAN 接口	必须操作。在**路由功能>>接口>>接口设置**页面中为 VLAN10, VLAN20 和 VLAN30 建立 VLAN 接口，分别为 192.168.10.1/24, 192.168.20.1/24, 192.168.30.1/24。
3	启用 DHCP 服务器功能	必须操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中启用 DHCP 服务器功能。
4	配置 IP 地址池	必须操作。在**路由功能>>DHCP 服务器>>地址池设置**页面中为各 VLAN 接口配置 IP 地址池参数，以 VLAN10 为例，网络地址配置为 192.168.10.0，子网掩码为 255.255.255.0，网关配置为 VLAN 接口地址 192.168.10.1，DNS 服务器配置为 160.20.30.2，同时配置租约并为 IP 地址池命名等。
5	配置预留 IP 地址	必须操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中为每个 VLAN 中的固定计算机配置预留 IP 地址不做分配。

步骤	操作	说明
6	手动绑定 IP 地址	可选操作。在**路由功能>>DHCP 服务器>>静态绑定**页面中可以为特殊客户端指定特定的 IP 地址。

10.5 DHCP 中继

➢ **DHCP 中继的应用环境**

在 DHCP 的基本网络模型中，要求客户机和服务器处于同一个局域网，客户端设备通过广播的形式向服务器动态获取 IP 地址。这种模型要求每个网络中均需要配置 DHCP 服务器，这种方式无疑会提高网络建设成本。引入 DHCP Relay 可以有效解决这一问题。DHCP Relay 设备可以为不同网段间的 DHCP Client 和 DHCP Server 提供中继服务，将 DHCP 协议报文跨网段转发，使得多个网络上的 DHCP Client 可以共享一台 DHCP Server。

➢ **DHCP 中继在 T3700G-28TQ 上的实现**

下图为我司交换机 T3700G-28TQ 配置为 DHCP 中继时的网络拓扑图示例，具体的应用环境可能根据实际需求有所调整。

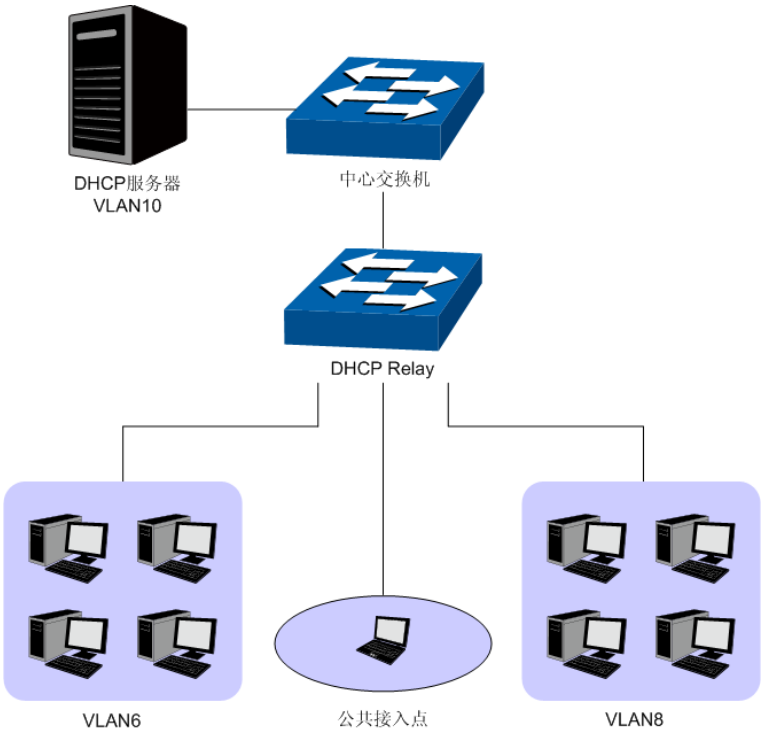


图 10-13 DHCP 中继典型拓扑图

为了保证所有 VLAN 中的设备能够安全顺利的获得 IP 地址，工作在 DHCP 中继模式的 T3700G-28TQ 交换机为多个 VLAN 与服务器之间转发 DHCP 协议报文，使所有 VLAN 中的设备均能够从网络中的 DHCP 服务器获得 IP 地址。

- 当交换机收到来自客户端的 DHCP-DISCOVER 和 DHCP-REQUEST 报文时，在报文中的 giaddr 字段写入接收端口的接口 IP 地址，同时插入可选项 option82，并以单播的形式将报文转发给指定的 DHCP 服务器；
- 当收到来自服务器的应答报文时，交换机将删除数据包中的 option 82 字段，将 DHCP 应答报文向中继设备的接口网络中广播。

详细的报文交换过程请参考下图，其中(B)表示广播，(U)表示单播。

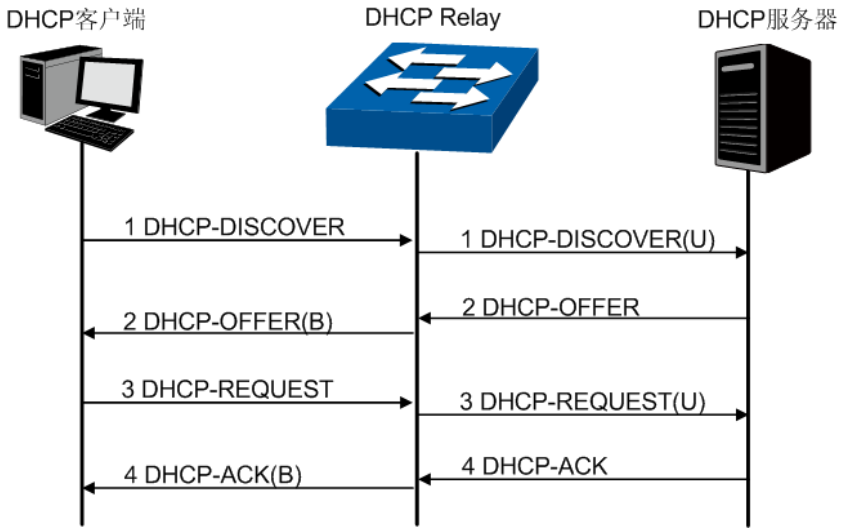


图 10-14 报文交互过程图片

- **DHCP Relay 在 T3700G-28TQ 上的配置要点**

1) 配置 Option 82 参数。关于 Option 82 选项的详细说明请参考下一节。建议在最靠近 DHCP 客户端的 Relay 设备上启用 Option 82 功能，以便精确记录客户端位置信息。

2) 配置 DHCP Server 信息。

- **中继代理选项 Option 82**

在我司交换机上，Option 82 被定义为中继信息选项，用于记录 DHCP 客户端的位置信息，常见的信息有 VLAN 信息、连接端口。当在交换机上配置了 Option82 选项时，交换机在接收到的 DHCP-DISCOVER 和 DHCP-REQUEST 报文中添加 Option 82 字段标记客户端信息，并转发给 DHCP 服务器。DHCP 服务器可以从 Option 82 字段中获得相关信息，并执行相应的分配策略，实现对客户端的安全和计费等控制。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。

目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 请求报文的所属 VLAN 以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 请求报文的 DHCP Relay 设备的 MAC 地址，填充格式如下图所示。同时，也支持自定义电路 ID 子选项和远程 ID 子选项。

下图为缺省情况下我司交换机定义的 option 82 填充格式，括号中的数字表示该字段的字节数。如图所示，缺省情况下，子选项 1 为电路 ID 子选项，其填充内容为 2 个字节的 VLAN 参数和 2 个字节的接收端口。子选项 2 为远程 ID 子选项，其填充内容为 6 个字节的客户端 MAC 地址。同时用户也可以自定义的两个子选项填充值。

option82	Length(1)		
sub-option1(1)	Length(1)	VLAN(2)	Port(2)
sub-option2(1)	Length(1)	Hardware address(6)	

图 10-15 option 82 字段格式

注意:

Option82 的配置参数需要结合并满足网络需求。

通过DHCP中继功能，交换机能在不同的VLAN或子网中获取IP地址。在特定的VLAN中指定DHCP服务器，开启 DHCP 中继功能并指定服务器的地址，在其他 VLAN 的设备就能获取 IP 地址。DHCP 中继功能可以减少网络中 DHCP 服务器的数量。

DHCP 中继功能包括**全局配置**和 **DHCP 服务器**两个配置页面。

10.5.1 全局配置

DHCP 中继功能在 DHCP 服务器功能开启后生效(开启 DHCP 服务器功能见 10.4.1 DHCP 服务器)，本页面用于配置 Option 82 选项来辅助 IP 地址分配。

进入页面的方法：**路由功能>>DHCP 中继>>全局配置**

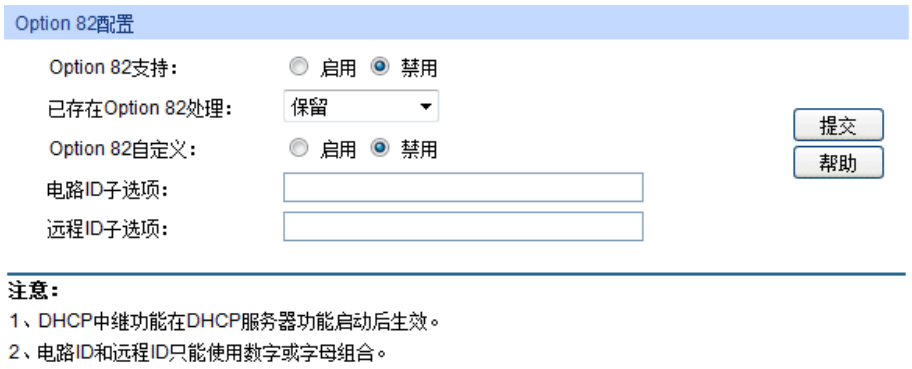


图 10-16 DHCP 中继全局配置

条目介绍：

- **Option 82 设置**

Option 82 支持：	选择是否启用 Option 82 字段。默认关闭。
已存在 Option 82 处理：	当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。 ● 保留：保留数据包中的 Option 字段信息。 ● 替换：替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。 ● 丢弃：丢弃包含 Option 82 字段的数据包。
Option 82 自定义：	开启或关闭 Option82 自定义功能，添加自定义的 Option 82 信息。
电路 ID 子选项：	输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。
远程 ID 子选项：	输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

10.5.2 DHCP 服务器

本页面用来配置 DHCP 服务器的相关参数。

进入页面的方法：**路由功能>>DHCP 中继>>DHCP 服务器**

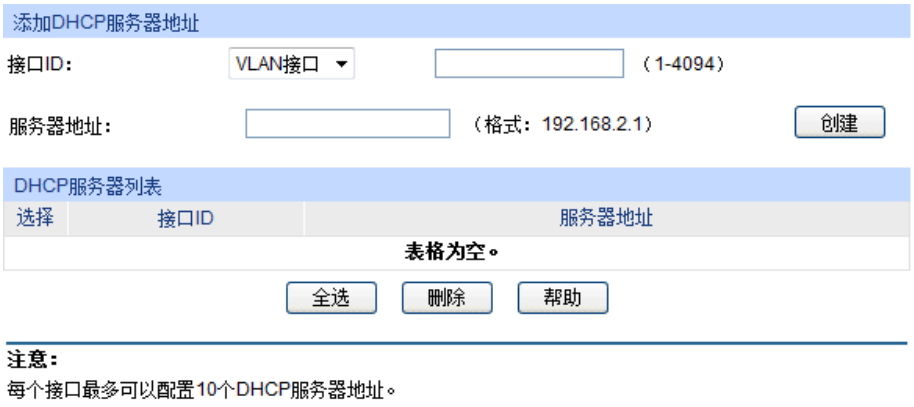


图 10-17 DHCP 服务器

条目介绍：

- **添加 DHCP 服务器地址**

  接口 ID： 选择接口类型，并输入对应接口号。

  服务器地址: 填写 DHCP 服务器的 IP 地址。

- **DHCP 服务器列表**

  选择： 勾选 DHCP 服务器条目进行删除，可多选。

  接口 ID： 显示 DHCP 服务器的接口 ID。

  服务器地址： 显示 DHCP 服务器的 IP 地址。

DHCP 中继配置步骤：

步骤	操作	说明
1	启用 DHCP 中继功能。	必选操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**功能页面中启用 DHCP 中继功能。
2	配置 Option 82 选项。	可选操作。在**路由功能>>DHCP 服务器>>全局配置**功能页面中配置 Option 82 选项参数。
3	配置 DHCP Server。	必选操作。在**路由功能>>DHCP 中继>>DHCP 服务器**功能页面中配置 DHCP 服务器来提供 IP 分配服务。

10.6 代理 ARP

代理 ARP 是 ARP 协议的一种应用。通常应用于网关在连接不同网络时，为不同网络中的计算机提供 ARP 代理服务。网关收到源计算机向目标网络计算机发送的 ARP 请求时，使用自己的 MAC 地址与目标计算机的 IP 地址对源计算机进行 ARP 应答，使得不同网络中的计算机能够正常通信而不必关心网络的划分。

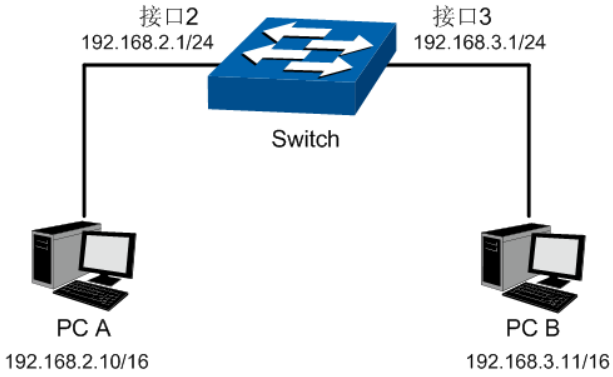
代理 ARP 多应用于下列两种环境：

1) 当不同网络中没有配置缺省网关的计算机要和其他网络中的计算机实现通信，其通过发送的 ARP 请求报文来试图通信，而网关在收到该 ARP 请求报文时，其代理 ARP 机制将代替目标计算机进行 ARP 应答，并为两个网络转发通信报文。

2) 当对网络进行 VLSM 子网划分时，可通过在网关上配置 ARP 代理，使得网络中计算机原有网络参数配置不做相应变更也可以进行通信。这种应用环境将在接下来的内容中详细介绍。

➢ **代理 ARP 工作机制**

上述两种代理 ARP 的应用环境可以简化为下图所示案例。



如图所示，由于PC A(192.168.2.10/16)与PC B(192.168.3.11/16)处于同一网段，当PC A需要与PC B通信时，会以广播方式发送ARP请求报文请求PC B的MAC地址。如果A、B分别属于不同的VLAN，则请求报文不能到达B，双方不能正常通信。当交换机开启了代理ARP功能后，接口2收到ARP请求报文时，发现ARP请求报文指向了另一个网络，则交换机会以接口2的MAC地址发送ARP应答报文给PC A。PC A收到伪应答报文后建立ARP表项，表项中PC B的IP地址对应着接口2的MAC地址。后续PC A发给PC B的报文都会发送到接口2，然后由交换机进行三层转发，从而实现A与B的通信。

10.6.1 代理 ARP

本页面用于配置代理 ARP 功能。**进入界面的方法：路由功能>>代理 ARP>>代理 ARP**

图 10-18 代理 ARP

条目介绍：

➢ **全局设置**

查找默认路由： 如果功能开启，在搜寻 ARP 代理时会搜索默认路由。

➢ **代理 ARP 信息**

选择： 选择要设置的表项，可多选。

IP 地址： 显示网络接口的 IP 地址。

子网掩码： 显示网络接口的子网掩码。

接口： 显示网络接口。

接口名称： 显示网络接口的接口名称。

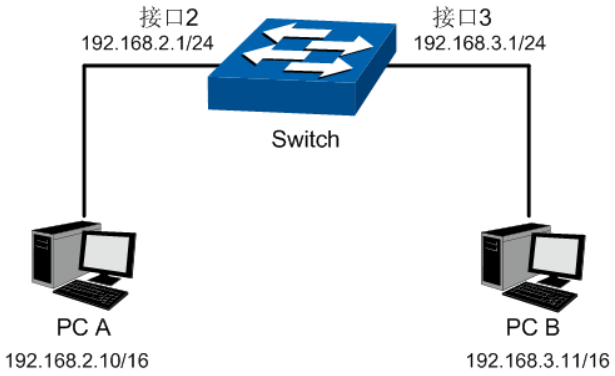
状态： 启用或禁用该接口上的代理 ARP 功能。

10.6.2 代理 ARP 功能的组网应用

- **组网需求**

1. PC A 和 PC B 在同一网段，PC A 的 IP 地址为 192.168.2.10/16，PC B 的 IP 地址为 192.168.3.11/16。
2. PC A 和 PC B 分别属于不同的子网 VLAN2 和 VLAN3。
3. 通过开启接口 2（192.168.2.1/24）和接口 3（192.168.3.1/24）的代理 ARP 功能实现 A、B 之间的通信。

- **组网图**



- **配置步骤**

- **配置交换机**

步骤	操作	说明
1	创建 VLAN2	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 2。
2	创建 VLAN3	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 3。
3	添加接口 2	在**路由功能>>接口>>接口设置**页面添加接口 2，IP 地址为 192.168.2.1，子网掩码为 255.255.255.0，VLANID 为 2，接口名称为 VLAN2。
4	添加接口 3	在**路由功能>>接口>>接口设置**页面添加接口 3，IP 地址为 192.168.3.1，子网掩码为 255.255.255.0，VLANID 为 3，接口名称为 VLAN3。
5	启用代理 ARP	在**路由功能>>代理 ARP** 页面启用接口 2 和接口 3 的代理 ARP 功能。

10.7 ARP

本页面用于显示 ARP 表，可以查看本机中所有的静态或动态 ARP 条目。

进入界面的方法：路由功能>ARP>>ARP 表

图 10-19 ARP 表

条目介绍：

- **ARP 表**

接口：	ARP 条目对应的网络接口。
IP 地址：	ARP 条目中的 IP 地址。
MAC 地址：	ARP 条目中 IP 对应的 MAC 地址。
类型：	ARP 条目类型，例如“静态”或者“动态”。
老化时间：	条目老化剩余时间。

10.8 RIP

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的动态路由协议，主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP作为最早的内部网关协议（Interior Gateway Protocol，IGP）之一，由于实现比较简单，在配置和维护管理方面也远比OSPF和IS-IS容易，至今仍被广泛使用。RIP当前有RIPv1和RIPv2两个版本。

RIP采用距离矢量（Distance-Vector）算法，使用跳数来度量到达目的地址的距离，并定义含有跳数最少的路径为最优路径。路由器到与它直接相连网络的跳数为0，每经过一个路由器，跳数就加1。跳数被称为度量值。为限制收敛时间，RIP规定度量值的取值范围为0-15之间的整数，数值16表示无穷大，即目的网络不可达。正是由于这个限制，RIP不适合应用于大型网络。

- **RIP 应用场景**

RIP允许的最大跳数为15，因此RIP适用于规模较小的网络，比如校园网以及结构较简单的地区性网络，如下图所示：

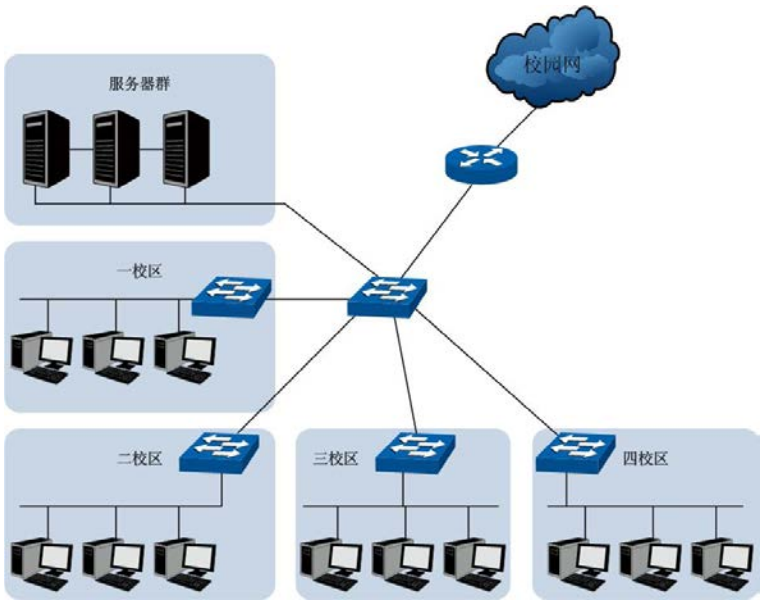


图 10-20 RIP典型应用场景

- **RIP 特性**

RIP有如下特性：

1) 设计单一。RIP 是典型的基于距离矢量（Distance-Vector）算法的动态路由协议，使用跳数作为度量值，并定义含有跳数最少的路径是最优路径。如果到相同目的站点有两条不同带宽的路径，但跳数相同，RIP 仍认为两条路径是等距离的。

2) 适用于规模较小的网络。RIP 规定度量值的取值范围为 0-15 之间的整数，数值 16 表示无穷大，即目的网络不可达。

3) RIP 是基于用户数据报协议（UDP）的协议。它通过 UDP 报文进行路由信息的交换，使用的端口号为 520。

4) 为提高性能，防止产生路由循环，RIP 支持水平分割和毒性逆转功能。

- **RIP 基本原理与实现**

RIP 要求路由器维护一个 RIP 路由表，该路由表记录了所有可达目的地的路由项。RIP 定期以广播形式（RIPv2 支持广播和组播两种方式）向所有邻居发送包含整个路由表的更新信息，并依赖邻居向它的邻居传递更新信息。其邻居路由器接收到这些信息后进行路由计算，更新路由表。

每条路由项都包含了如下信息：

- 目的网络：目的网络的 IP 地址和子网掩码。该 IP 地址和子网掩码共同决定了一个网络，到达该网络的报文可通过此路由条目进行转发。
- 下一跳地址：为到达目的网络，需要经过的相邻路由器的接口 IP 地址。
- 度量值：到达目的网络所需要的跳数。
- 接口名称：路由器转发报文通过的出接口。
- 老化时间：从路由条目最后一次被更新到现在所经过的时间。若该路由条目在超时计时器规定的时间内没有被更新，其跳数将被设为 16，表示网络不可达。

RIP 定义了两种报文类型：请求报文和响应报文（或称为更新报文）。

- 请求报文：向邻居路由器请求发送整个或部分路由表。

- 响应报文（更新报文）：可以是对邻居路由器的请求作出应答，也可以是主动向邻居路由器发送更新。

RIP 运行过程如下图所示：

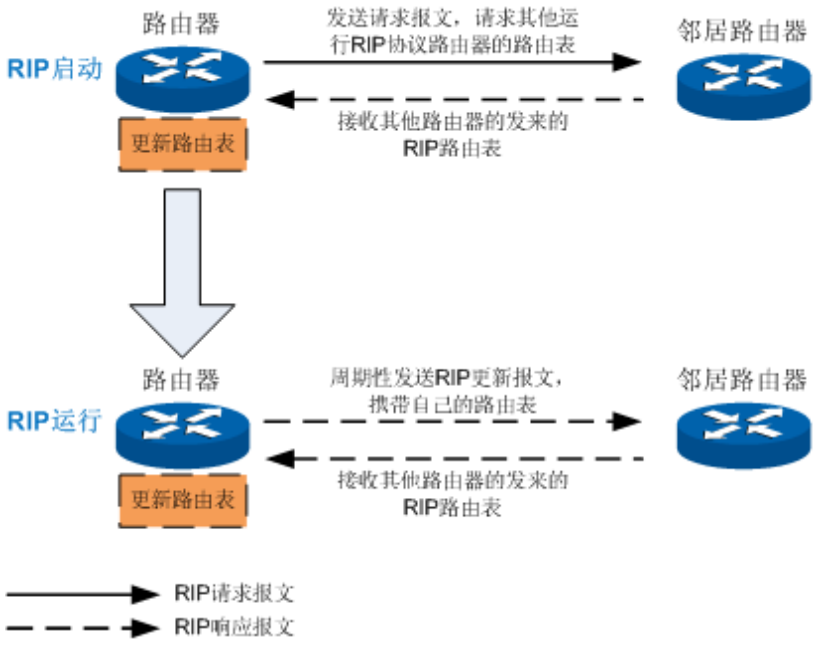


图 10-21 RIP 协议运行过程

1) RIP 路由表的形成

RIP 启动时的初始路由表中仅包含了本设备的一些直连接口路由信息。通过相邻设备互相学习路由表项，才能实现各网段路由互通。

a) RIP 初始化时，路由器会从每个启用 RIP 协议的接口广播请求报文。该请求报文包含当前路由器学习到的全部路由信息，即整个路由表，并向相邻设备请求完整的路由表。

b) 之后路由器不断地侦听来自其他路由器的 RIP 响应报文。接收到请求报文且启用 RIP 协议的邻居路由器会回送包含它们的路由表的响应报文。不关心路由更新信息的主机和其他设备则丢弃该请求报文。

c) 当发出请求报文的路由器收到响应报文时，它将开始处理附加在响应报文中的路由信息。对本地 RIP 路由表中尚未记录的路由表项，路由器直接将该路由信息添加到本地 RIP 路由表中；对本地已记录的路由表项，则按如下规则处理：

- 如果已有表项和新表项的来源接口相同，则无条件地根据最新路由信息更新本地路由表；
- 如果已有表项和新表现的来源接口不同，则比较它们的度量值，将度量值较小的作为自己的路由表项，如果度量值相同，则保留旧的表项。

这样，经过一段时间的路由信息收集以及更新，路由器就可以通过相邻设备收集整个网络的全部信息，完成网络收敛。

2) RIP 的更新与维护

为了应对网络拓扑变化，RIP 采用定期更新和老化机制来保证 RIP 路由表的实时性、有效性以及稳定性。RIP 协议在更新和维护路由信息时主要使用三个定时器，具体如下：

a) 更新计时器：路由器启动后，按照固定的时间间隔从每个启动 RIP 协议的接口广播更新报文（RIPv2 支持广播和组播两种方式发出更新报文）。该时间间隔由更新计时器决定，通常是 30

秒。更新报文包含了路由器的整个路由表。每个路由器的更新定时器都独立于网络中其他路由器，因此它们同时广播的可能性很小。

b) 超时计时器：路由器会为每一条新建的路由条目设置一个老化时间，如果路由器在老化时间内接收到该条目的更新报文，则保持该路由条目并将超时计时器初始化，重新计时；否则，该条目的跳数将被设置为 16，即目的网络不可达。该老化时间由超时计时器决定，通常是 180 秒即 6 个更新周期。

c) 垃圾回收计时器：路由器还为每条路由条目设置一个垃圾回收计时器，通常比超时计时器的时间长 60-240 秒。它定义了路由条目从跳数变为 16 到被清除的时间间隔。某个路由条目的超时计时器超时后，该条目的跳数将被设置为 16，如果到达垃圾回收计时器所规定的时间后，该路由条目仍没有得到更新，路由器将从路由表中彻底删除该条目。

3) 防止环路机制

RIP 是通过邻居之间相互通告自己的路由表来建立和维护 RIP 路由表的，路由器并不知道网络的全局情况，不仅收敛速度慢，还存在发生路由环路的可能。为提高性能，防止产生路由环路，RIP 增加了下列特性，最大限度避免环路的产生。

1) 计数到无穷：将度量值等于 16 定义为无穷大，即网络不可达。当发生路由环路时，在环路中循环的路由条目的度量值增加到 16 之后即被认为不可达，这样可以有效防止路由条目在环路中无休止地传输。该功能默认启用。

2) 水平分割：路由器不会把从某个接口学到的路由信息再从该接口发送回去。这样路由器就不会接收到由自身传达出去的路由信息，既减少了带宽消耗，又可以防止路由环路。

3) 毒性逆转：RIP 从某个接口学到路由条目后，会将该路由条目的度量值设为 16，再从原来的接口发送回去，收敛速度比水平分割更快。当同时启用水平分割和毒性逆转时，只有毒性逆转功能生效。

4) 触发更新：一旦某条路由的度量值发生了变化，路由器就会立刻向邻居路由器发布更新报文，而不是等到更新周期到来再发送。触发更新机制可以避免在多个路由器之间形成路由环路，同时也可以加速网络的收敛速度。

说明：

RIPv2 有两种更新报文传送方式：广播方式和组播方式。RIPv2 默认通过组播方式发送报文，使用的组播地址是保留的 D 类地址 224.0.0.9。当开启 RIPv2 广播功能时，RIPv2 使用广播方式代替组播方式来通告信息，以便 RIPv1 接收。

- **RIP 的版本**

RIP 包括 RIPV1 和 RIPV2 两个版本，1988 年 RFC 1058 对 RIP 协议做了说明，后来被称为 RIPv1。1998 年，IETF 推出了 RIP 改进版本的正式标准 RFC 2453，即 RIPv2。需注意的是，RIPv2 不是 RIPv1 的替代，而是在 RIPv1 协议的基础上增加了一些扩展特性，应用更加灵活，以适用于现代网络的路由选择环境。

1) RIPv1

RIPv1 是有类别路由协议，只支持以广播方式发布协议报文。RIPv1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类自然网段的路由，因此 RIPv1 不支持不连续子网。

2) RIPv2

RIPv2 同 RIPv1 相比，是无类别路由协议，支持可变长子网掩码、报文认证、无类域间路由、外部路由标记和组播。在这些拓展特性中，最重要的就是路由选择更新条目增加了子网掩码的字段，因

而 RIPv2 协议可以使用可变长的子网掩码，使其成为一个支持无类别路由选择的协议。拓展特性具体如下：

- 报文中携带自己的子网掩码信息，支持路由聚合和无类域间路由；
- 路由选择更新具有认证功能，能够验证某个路由选择更新报文的源的合法性；
- 报文中携带下一跳地址，在广播网上可以找到最优下一跳接口地址；
- 支持外部路由标记；
- 支持组播路由发送更新报文，减少资源消耗。

3) RIPv1 与 RIPv2 的兼容性

RIP 的协议规范充分考虑到 RIP 不同版本之间的兼容性。规范中约定如果 RIP 报文的版本字段值为 1 且报文中其他的未使用字段为非 0，那么 RIP 报文将被丢弃；如果版本字段值大于 1，那么 RIP 报文将会被处理，不过该报文中被 RIPv1 定义为未使用的字段将被忽略。因此，RIPv2 这种新协议版本可以向后兼容 RIPv1。

➢ RIP 报文

1) RIPv1 的报文格式

RIPv1 报文由头部和多个路由条目组成（一个 RIP 报文最多可以有 25 个路由条目）。报文头部包含一个命令标识和一个版本号。每个路由条目包含地址族标识、路由可达的 IP 地址和路由的跳数。如果某台路由器必须发送多于 25 条路由的更新报文，那么必须产生多条 RIP 报文。RIPv1 报文格式如图 10-22 所示：

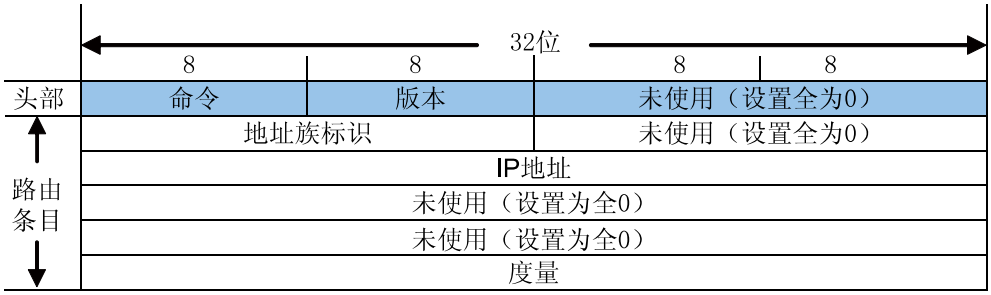


图 10-22 RIPv1 的报文格式

各字段的解释如下：

- 命令：取值 1 或 2，用以标识报文的类型。1 表示该报文为请求报文，2 表示该报文为响应报文。
- 版本：RIP 的版本号。取值 0x01，表示 RIPv1。
- 地址族标识：对于 IP 协议，该字段取值为 2。
- IP 地址：路由条目的目的 IP 地址，该字段可以是自然网段地址、子网地址或主机地址。
- 度量：即跳数，取值范围为 0-16。

2) RIPv2 的报文格式

RIPv2 的报文格式与 RIPv1 类似，所有相对于原来协议的拓展特性（路由标记，子网掩码和下一跳）都是由未使用的字段提供的，如图 10-23 所示。

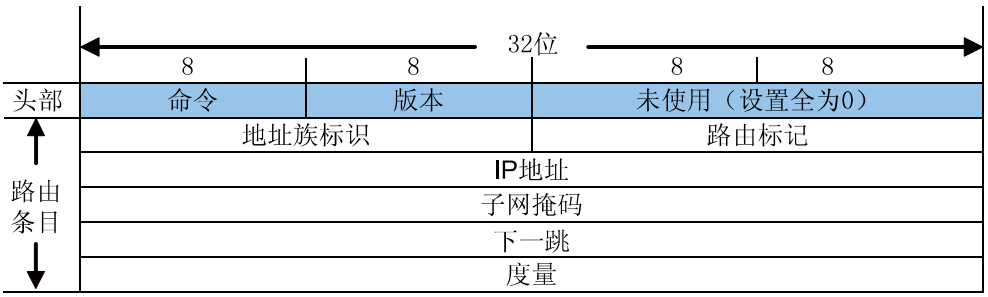


图 10-23 RIPV2 的报文格式

其中，与 RIPv1 不同的字段的解释如下：

- 版本：RIP 的版本号。取值 0x02，表示 RIPv2。
- 路由标记：用于支持外部网关协议。默认的情况是使用这个字段携带 RIP 引入的外部路由协议的路由的自主系统编号。如果使用 RIP 协议的路由器收到的路由条目中，该字段为非零，则直接向外通告该路由信息，如果该字段没有值，则需将该字段的值改为 0 再向外通告。RIP 协议本身并不使用这个字段。
- 子网掩码：是一个 32 位的掩码，用来标识 IPv4 地址的网络和子网部分。
- 下一跳：如果存在，它标识一个比发布此条路由信息的路由地址更优的下一跳地址。如果该字段为全 0（0.0.0.0），则表示发布此条路由信息的路由地址就是最优下一跳地址。

3) RIPv2 的认证报文格式

RIPv2 为了支持报文认证，使用第一个路由条目作为认证项，因此在含有认证的单个 RIPv2 响应报文中，最多可以携带的路由条目只有 24 条。RIPv2 通过将地址族标识字段的值设为 0xFFFF 标识报文携带认证信息。RIPv2 的认证报文格式如图 10-24 所示。

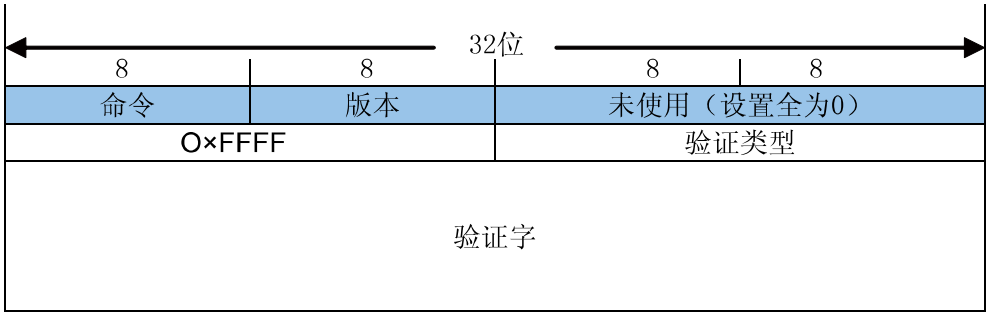


图 10-24 RIPv2 的认证报文格式

各字段的解释如下：

- 验证类型：取值 2 或 3。值为 2 时表示简单认证，值为 3 时表示 MD5 认证。
- 验证字：当使用简单认证时包含密码信息（密钥）；当使用 MD5 认证时包含密钥 ID 和密钥。该字段长度为 16 个八位组字节。

➢ **交换机特性**

1) 支持 RIPv1 和 RIPv2

本交换机同时支持 RIPv1 和 RIPv2 两种版本的协议，您可以根据实际的网络需求设置，以提高网络性能。

2) 自动汇聚

自动汇聚的原理是，同一个自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一个网段的路由发送。RIPv1 的协议报文中没有携带掩码信息，故 RIPv1 发布的就是自然掩码的路由。

RIPv2 支持自动汇聚，因为 RIPv2 报文携带掩码位，所以支持子网划分。在 RIPv2 中进行自动汇聚可提高大型网络的可扩展性和效率，缩减路由表。

本交换机支持基于 RIP 进程的有类聚合：聚合后的路由使用自然掩码的路由形式发布，RIPv2 聚合是按类聚和的，聚合得到最优的度量值。比如，对于 10.1.1.0 /24（度量值为 2）和 10.1.2.0 /24（度量值为 3）这两条路由，会聚合成自然网段路由 10.0.0.0 /8（度量值为 2）。但在启用了水平分割或毒性逆转的情况下，有类聚合将失效，这是因为水平分割或毒性逆转将抑制一些路由的发布，配置了有类聚合时一条聚合路由可能是聚合了从不同的接口上学到的路由，这样在向外发布时就会产生冲突。

3) 引入外部路由

在本交换机上，RIP 不仅可以通过与邻居交换路由表学习路由信息，还可以引入其他进程或其他协议例如 OSPF 和静态路由学到的路由信息，从而丰富路由表项。

4) 路由重新分配

当路由器使用路由选择协议通告从其他方式学习到的路由时，路由器将执行重新分配。这里所谓的其他方式可能是另外一个路由选择协议、静态路由或直连目标网络。例如路由器可能同时运行静态路由进程和 RIP 进程。如果设置 RIP 进程通告来自静态路由进程的路由，这就叫做重新分配静态路由。IP 路由选择协议的能力相差非常大，对路由重新分配影响最大的协议特性是度量值和管理距离的差异性。

RIP 默认度量值：执行路由重新分配的路由器将为被重新分配的路由指派度量值。例如，运行 RIP 协议的路由器引入外部 OSPF 路由，路由器会为 OSPF 路由重新分配度量值，然后向其他运行 RIP 的路由器通告这些路由。在本交换机上，RIP 协议在引入外部路由时，为其重新分配的度量值默认为 12。

RIP 管理距离：当路由器正在运行多个路由选择协议，并从每个协议都学习到一条到达相同目标网络的路由。由于每一个路由选择协议均使用自己的度量方案定义最优路径，例如 RIP 使用跳数，而 EIGRP 使用带宽和时延，使得路由器无法通过比较度量值来选择最优路径。为了判断最优路径，各路由协议都被赋予了一个管理距离。管理距离被看作是一个可信度测度，管理距离的数值越小，协议的可信度越高。其中 255 表示任何来自不可信源端的路由。在本交换机上，RIP 的管理距离默认为 120。

RIP 模块主要用于配置交换机的 RIP 功能，包括**基本配置、接口配置**以及**路由表**三个部分。

10.8.1 基本配置

本页面用于开启全局 RIP 功能，配置 RIP 的全局属性以及使能和查看开启 RIP 协议的网段。

进入界面的方法：**路由功能>>RIP>>基本配置**

图 10-25 基本配置

条目介绍：

- **全局配置**

RIP 协议： 选择启用或禁用交换机的 RIP 该功能，默认为“禁用”。

RIP 版本： 选择使用的 RIP 协议版本，可选版本有 RIPv1 和 RIPv2。

- Default：仅发送 RIPv1 报文，但可接收 RIPv1 和 RIPv2 报文。
- RIPv1：仅发送和接收 RIPv1 报文。发送报文时采用广播方式。
- RIPv2：仅发送和接收 RIPv2 报文。发送报文时采用组播方式。

RIP 距离： 配置 RIP 协议的管理距离。取值范围为 1-255。管理距离被看作是一个可信度测度，管理距离数值越小，协议的可信度越高。其中 255 表示任何来自不可信源端的路由。默认为“120”。

RIP 自动汇聚： 选择启用或禁用 RIP 路由条目的自动汇聚功能。如果启用该功能，多条路由条目在网络边界可以汇聚为一条路由条目，起到减小发送的路由条目的作用。默认为“禁用”。

默认度量值： 设置 RIP 协议在引入外部路由时的默认度量值，取值范围为 1-15，默认值为“1”。

引入外部静态路由： 选择使能或者禁用引入外部静态路由到 RIP 协议中，默认为“禁用”。

引入外部 OSPF 路由： 选择使能或者禁用引入外部 OSPF 路由到 RIP 协议中，默认为“禁用”。

引入静态路由度量值： 设置 RIP 协议在引入外部静态路由时的默认度量值，取值范围为 0-15。默认值为 “0”，表示不使用外部静态路由。

引入 OSPF 路由度量值： 设置 RIP 协议在引入外部 OSPF 路由时的默认度量值，取值范围为 0-15。默认值为 “0”，表示不使用外部 OSPF 路由。

更新计时器： 填写 RIP 任务发送更新报文的间隔。取值范围为 1-100 秒，推荐设置为“30 秒”。

超时计时器： 填写路由条目的有效期，如果在此段时间内该条目未被更新，那么该条目所表达的路径将被自动设置为不可达。取值范围为 1-300 秒，推荐设置为“180 秒”（即 6 个更新周期）。

垃圾回收计时器： 垃圾回收计时器决定了路由条目从变为不可达到被彻底删除的时间间隔，如果一条路由条目变为不可达以后，并且在该段时间内仍未被更新，那么该条目将会被自动删除。取值范围为 1-500 秒，推荐设置为“120 秒”。

- **网段使能**

添加网段： 用于添加使能 RIP 协议的网段，是将交换机的接口开始 RIP 功能的唯一方法。添加一个网段之后，在该网段中的交换机接口将启动 RIP 协议。格式为 192.168.0.0。

- **RIP 网段列表**

选择： 列表中为已经使能 RIP 协议的网段，可勾选需要删除的条目并点击<删除>按钮进行删除，可多选。

已经添加网段： 显示已经使能 RIP 协议的网段。

说明：

- 交换机默认情况下使用 RIPv1 版本协议，接收和发送 RIPv1 版本的报文。如果需要修改交换机接口接收和发送 RIP 报文的版本，请在**路由功能>>RIP>>接口配置**进行相关配置。
- 如果连接的网络是不连续子网，建议您禁用 **RIP 自动汇聚**。

RIP 全局配置步骤：

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面选择启用 RIP 协议。
2	使能网段	必选操作。在**路由功能>>RIP>>基本配置**页面的网段使能部分，添加网段，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

10.8.2 接口配置

本页面用于配置和查看运行 RIP 协议的接口及其运行参数。

进入界面的方法：**路由功能>>RIP>>接口配置**

图 10-26 接口配置

条目介绍：

- **接口配置**

选择： 勾选需要修改运行参数的接口，可多选。

目的地址/子网掩码： 显示接口的 IP 地址和子网掩码。

接口状态： 显示接口的 RIP 运行状态，由 RIP 使能的网段决定。

RIP 发送版本： 选择接口所支持的发送报文的 RIP 版本号。

- RIPv1：发送报文使用 RIPv1 格式。
- RIPv2：发送报文使用 RIPv2 格式。

RIP 接收版本： 接口所支持的接收报文的 RIP 版本号。

- RIPv1：支持接收 RIPv1 格式的报文。
- RIPv2：支持接收 RIPv2 格式的报文。
- Both：同时支持接收 RIPv1 和 RIPv2 格式的报文。

RIPv2 广播： 选择是否启用 RIPv2 广播特性。启用以后，接口将使用 RIPv2 的报文格式，发送广播报文，以及接收广播和多播报文。

被动接口： 抑制接口发送路由更新报文。

认证类型： 设置接口所接收和发送的报文是否使用认证功能，默认为“无”。只有使用相同认证类型和认证密码的设备能交换 RIP 报文。仅 RIPv2 支持报文认证功能。

- 无：不使用认证功能。
- 简单认证：使用简单密码进行认证。选择“简单认证”后，需要在“密钥”一栏输入认证时使用的密钥。该密钥将被添加在 RIP 报文首部，只有使用相同认证类型和密钥的设备能相互通信。
- MD5：使用 MD5 进行认证。选择“MD5”后，需要在“密钥 ID”和“密钥”栏中输入认证时使用的密钥 ID 和密钥。

密钥 ID: 设置 MD5 密钥时必须同时输入密钥 ID，该 ID 为 1-255 之间的一个整数。

密钥： 设置接口认证时使用的密匙。该密钥为一个字符串。

水平分割： 选择是否启用水平分割功能。启用以后，本设备不会把从某个接口学到的路由信息再从该接口发送回去。默认为“启用”。

毒性逆转： 选择是否启用毒性逆转功能。启用以后，RIP 从某个接口学到路由条目后，会将该路由条目的度量值设为 16，再从原来的接口发送回去。当同时启用水平分割和毒性逆转时，只有毒性逆转功能生效。该功能默认为“禁用”。

说明：

- 当 RIP 接收版本和发送版本的全局配置与接口配置不一致时，将以接口配置为准。
- RIPv1 不支持报文认证，因此当 RIP 版本号选择为 RIPv1，配置的认证信息（认证类型，密钥 ID 和密钥）不生效。当 RIP 的版本为 RIPv1 时，虽然在接口视图下仍然可以配置验证方式，但由于 RIPv1 不支持认证，因此该配置不会生效。
- RIPv2 默认通过组播方式发送更新报文，使用的组播地址是保留的 D 类地址 224.0.0.9。当开启 RIPv2 广播功能时，RIPv2 使用广播方式代替组播方式来通告信息，以便 RIPv1 可以接受它们。

10.8.3 路由表

RIP 路由表为 RIP 协议独立维护的路由表，记录了通过 RIP 协议产生的路由信息。本页面用于显示目前通过 RIP 协议生成的路由信息。

进入界面的方法：**路由功能>>RIP>>路由表**

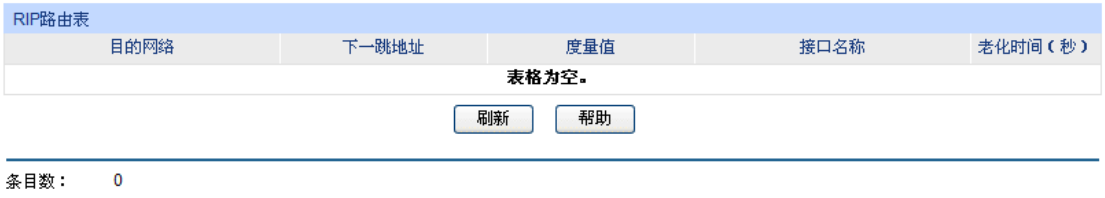


图 10-27 RIP 路由表

条目介绍：

➢ **RIP 路由表**

目的网络： 显示目的网络的 IP 地址和子网掩码。该 IP 地址和子网掩码共同决定了一个网络，到达该网络的报文可通过此路由条目进行转发。

下一跳地址： 显示为到达目的网络，需要经过的相邻路由器的接口 IP 地址。

度量值： 显示到达目的网络所需要的跳数。

接口名称： 显示对路由条目所指定的报文进行转发的接口名称。

老化时间： 显示从路由条目最后一次被更新到现在所经过的时间。若该路由条目未被更新，到达超时计时器所规定的时间后，其度量值会被设为无穷大；到达垃圾回收计时器所规定的时间后，路由条目将被删除。

10.8.4 RIP 的组网应用

➢ **组网需求**

1. 交换机 A 三个接口的 IP 地址分别为 1.1.1.1/24，2.1.1.1/24，3.1.1.1/24。交换机 B 三个接口的 IP 地址分别为 1.1.1.2/24，10.1.1.1/24，11.1.1.1/24。
2. 要求在交换机 A，B 的所有接口上使能 RIP，并使用 RIPv2 协议进行网络互连。

➢ **组网图**

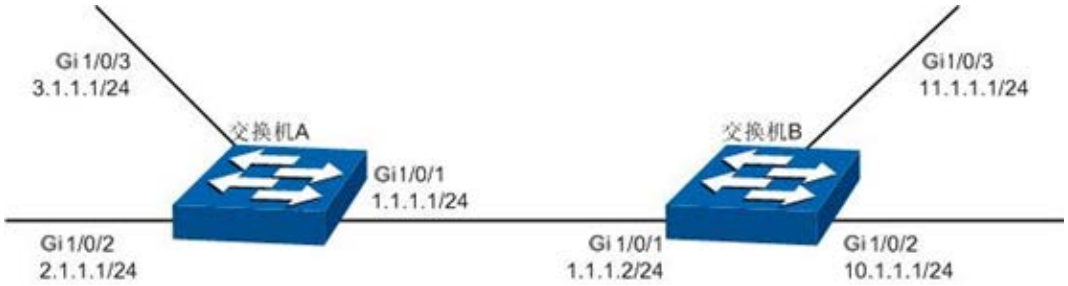


图 10-28 组网图

➢ **配置步骤**

- **配置交换机 A**

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面启用 RIP 协议，选择 RIP 版本为 RIPv2。
2	使能接口所在网段	必选操作。在**路由功能>>RIP>>基本配置**页面的网段使能部分，添加网段 1.0.0.0，2.0.0.0，3.0.0.0，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

- **配置交换机 B**

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面开启 RIP 协议，选择 RIP 版本为 RIPv2。
2	使能接口所在网段	必选操作。在**路由功能>>RIP>>基本配置**页面网段使能部分，添加网段 1.0.0.0，10.0.0.0，11.0.0.0，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

10.9 OSPF

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF 组织开发的一个基于链路状态的路由选择协议，也是 IETF 组织建议使用的内部网关协议。目前针对 IPv4 网络中使用的 OSPF 协议标准是 OSPF Version 2，在 RFC 2328 中有详细的定义，本说明书中将概括地介绍 OSPF Version 2。

➢ **OSPF 概述**

1. OSPF 特性

OSPF 协议作为在网络搭建中常用的路由选择协议，具有如下特性：

- 快速收敛，在网络拓扑发生变化后立即发送更新报文，使自治系统中的路由能够快速同步更新。
- 由于具有快速收敛特性，因此 OSPF 路由协议在大规模的网络中拥有快速稳定的表现，且不容易受到有害路由信息的影响。

- OSPF 协议引入区域的概念，将自治系统划分成区域来管理，使得区域内路由器只需和同区域的路由器保持链路状态数据库同步，链路状态数据库大小的缩减降低了对路由器内存的消耗，而路由信息的减少也释放了路由器的 CPU 资源，同时也减少了路由信息占用的网络带宽。
- OSPF 协议支持到同一目的地址的多条等价路由进行负载均衡，实现更高效率的数据转发。
- 支持可变长子网掩码 VLSM 路由寻址。
- 支持基于接口的报文验证，以保证报文交互和路由计算的安全性。
- 在特定网络类型的链路上使用保留的组播地址来减少对其他无关路由设备的影响。

2. OSPF 常用场景

OSPF 协议一般用于大型复杂的网络环境中。下图是一个大型公司的网络实例图。在大型网络中，按部门进行网络区域划分，路由器之间使用 OSPF 协议作为基本路由协议，这样既能够保证区域信息的交互，又能够保证各部门之间的网络独立。

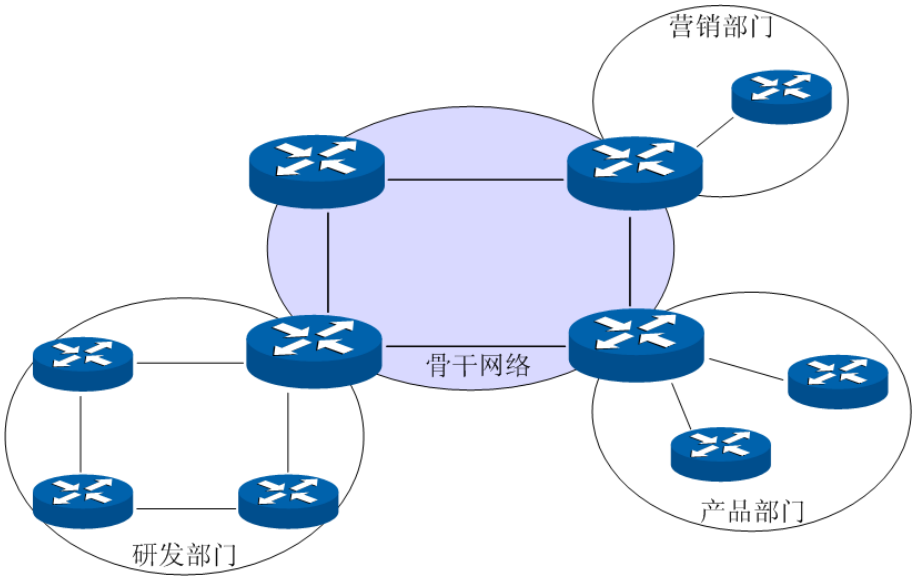


图 10-29 OSPF 路由协议常用场景

在自治系统规模较大时，拓扑结构发生变化的概率也增大，任意一台路由器进行网络调整都会使网络处于不稳定状态，造成大量的 OSPF 协议报文在网络中重复转发，所有的路由器都需要重新计算路由，浪费网络资源。通过划分区域（Area）可以有效解决此类问题。路由器仅需要和它所在的区域内的其他路由器维护相同的链路状态数据库，然后由区域边界路由器(ABR)汇总不同区域的路由信息并向其他区域发布。详细的区域划分和路由器类型请查看后续章节说明。

➢ OSPF 基本原理

本节将详细介绍 OSPF 协议的工作原理，首先简单介绍 OSPF 路由协议相关的几个基本概念。

1. 自治系统（Autonomous System）

一组使用相同路由协议交换路由信息的路由器，缩写为 AS。OSPF 工作在一个自治系统范围内，是一种内部网关协议。

2. 路由器 ID

一台运行 OSPF 协议路由器通过定义路由器 ID 在网络中标识自己的唯一性，路由器 ID 是一个 32 比特无符号整数，可以由管理员手动配置也可以由路由器自动选举。为了避免自动选举时网络中多台路由器获得相同的路由器 ID，建议手动配置路由器 ID。

在 RFC 协议中建议了自动选举路由器 ID 的方式，其建议优先采用 loopback 接口的 IP 地址按照数值大小来作为路由器 ID，其次选择路由接口中数值最大的接口 IP 作为路由器 ID。由于 loopback 接口具有良好的稳定性，只要路由器启动就处于活动状态，因此可以保证路由器在每次重启后都能够自动选举出 loopback 接口 IP 地址作为路由器 ID，使得路由器 ID 对外始终不变。为保证路由器 ID 的唯一性，请手动配置路由器 ID 或 loopback 接口的 IP 地址。

自动选举时，路由器将首先选择路由器上所有 loopback 接口中数值最大的 IP 地址作为路由器 ID，如果路由器上没有预先定义的 loopback 接口，则选择所有物理接口中数值最大的接口 IP 地址作为路由器 ID。

3. OSPF 的网络类型

OSPF 是动态路由协议，工作在网络层，根据不同的数据链路层特性，OSPF 路由协议使用不同的工作机制。OSPF 路由协议的工作机制与网络类型的关系分为如下 4 种：

1) 广播（Broadcast）类型：当网络类型是 Ethernet、FDDI 时，OSPF 协议以组播形式发送 Hello、LSU 和 LSAck 报文，例如 Hello 报文以组播形式发送给网络中的其他 OSPF 路由器，目的地址为预留的 224.0.0.5，而其他路由器向 OSPF DR 发送的链路状态更新和链路状态确认数据则发送到预留的组播地址 224.0.0.6；在此类广播类型网络中 DD 和 LSR 报文以单播形式发送。

2) NBMA（Non-Broadcast Multi-Access，非广播多点可达网络）类型：当网络类型是帧中继、ATM 或 X.25 时，这些网络上的路由器需要通过额外的配置来发现邻居，OSPF 协议报文以单播形式发送。

3) P2MP（Point-to-MultiPoint，点到多点）类型：点到多点网络通常是由 NBMA 类型网络强制更改而成的。在该类型的网络中，Hello 报文以目标 IP 为 224.0.0.5 的组播形式发送，LSU 和 LSAck 报文以目标 IP 为 224.0.0.5 的组播或单播形式发送，DD 和 LAR 报文以单播形式发送。

4) P2P（Point-to-Point，点到点）类型：当链路层协议是 PPP、HDLC 时，链路上总是连接一对路由器，建立有效邻居后通常可以形成邻接关系。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

我司交换机为以太网交换机，所有的接口网络类型默认为 Broadcast，同时也支持配置为可以自动发现邻居的 P2P 类型。为保证多点接入网络的连通性，请谨慎配置接口网络类型。在后续说明中将重点以广播类型接口介绍 OSPF 协议工作机制。

4. DR/BDR

在广播型网络和 NBMA 网络中，通常有多台同时运行 OSPF 协议的路由器，任意两台路由器之间建立邻居关系将会产生大量的邻接关系，当某一路由发生变化时会导致路由更新信息多次传递，浪费网络资源。

OSPF 协议定义的指定路由器 DR（Designated Router）和备份指定路由器 BDR（Backup Designated Router），由 DR 和 BDR 维护整个网络，其他路由器只与 DR 和 BDR 建立邻接关系，DR 向所有邻居泛洪扩散网络中的路由信息。当 DR 失效时，BDR 将成为新的 DR，避免了 DR 失效时网络重新选举 DR 期间网络不通。当然此时需要重新选举一个新的 BDR，虽然一样需要较长的时间，但并不影响通信过程。DR 和 BDR 具有稳定性，当一个网络中的 DR 和 BDR 确定了以后，即使有新路由器加入或者退出也不会重新选举，除非 DR 和 BDR 失效。

如下图所示，一个有五台路由器的网络中两两建立邻接关系，则需要建立 10 个邻接关系，邻接关系与路由器数量的关系为 N*(N-1)/2。如果启用 DR/BDR 的方式，则只需要建立 7 个邻接关系，邻接关系与路由器数量的关系为(N-2)*2+1。网络中的路由器数量越大，优越性将更加明显。

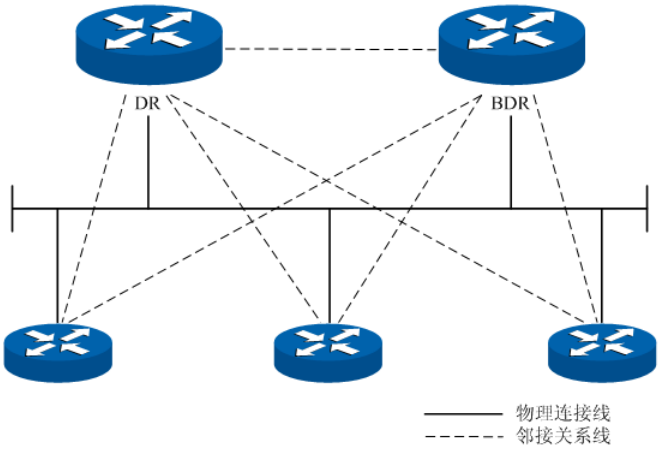


图 10-30 DR/BDR 邻接关系图

DR/BDR 的确定由接口优先级、路由器 ID 决定。首先根据接口优先级来判定一台路由器在相应接口接入的网络中是否能够成为 DR/BDR，优先级最高的将被选为 DR/BDR；当所有接口优先级相同时则根据路由器 ID 来判定。综上所述，DR/BDR 是路由器某个接口的特性，其表明路由器在某个网段中的地位，而不是路由器在网络中的特性，每个网段均需要选举 DR/BDR 来完成路由信息同步过程，配置路由接口时则需要根据网络规划来配置相关的接口参数。

- **OSPF 工作过程**

下面以两台初步启动接口 OSPF 协议的路由器为例，概括介绍 OSPF 路由协议在以太网模型中的工作过程。

1) 路由器接口启动了 OSPF 协议后，处于同一网段的接口将通过 Hello 报文发现邻居。如果接口连接到同一条公共数据链路，且接口的区域 ID、认证信息、网络掩码、Hello 时间间隔和邻居失效时间间隔（router dead-interval）相匹配，那么两台路由器就将对方加入自己的邻居列表。

2) 如果接收端路由器在 Hello 报文中的邻居列表发现了自己的 ID，则认为双向通信建立成功。随后将根据接口优先级、路由器 ID 等参数选举 DR/BDR，如果网络中已存在 DR/BDR 时，接受已经存在的 DR/BDR。

3) 确定 DR/BDR 后，网络中的路由器和 DR/BDR 之间两两选举出主从路由器，并开始同步链路状态数据库。

4) 网络中的路由器会与 DR/BDR 相互发送单播的链路状态通告 LSA，直到所有的路由器形成相同的链路状态数据库。同步数据链路数据库的过程中，如果发送方发出的数据库描述报文中包含接收方没有的或更新的 LSA，接收方将向发送方请求该 LSA 的详细内容。请求方通过 LSR 报文来请求具体的 LSA。即 DD 交换过程的任意阶段，只要接收的 DD 报文中包含更新的 LSA 信息，即可向对方发出 LSA 请求进行同步。收到 LSR 报文的路由器，会以单播形式向对端发送携带 LSA 的 LSU 报文。

5) 当两台路由器的链路状态数据库同步完成后，就形成了完全邻接关系。

6) 当区域内路由器的链路状态数据库完全相同时，每一台路由器都将以其自身为根，使用 SPF 算法来计算一个无环路的拓扑图，以描述它所知道的每一网络节点的最短转发路径，并根据最短转发路径拓扑图中构建出路由表为数据转发提供依据。

7) 路由表建立完成后，如果网络保持稳定，邻居之间将通过定期发送 Hello 报文保持邻居间的 keep-alive，而具有邻接关系的路由器则通过周期性的 LSA 更新来重新计算路由表以维护有效的路由表条目。

8) 当网络中有新加入的路由器时，将接受现有的 DR/BDR，并与 DR/BDR 同步链路状态数据库直到建立完全邻接关系。在同步链路状态数据库过程中，DR/BDR 从新加入的路由器获得 LSA，DR 将把这个 LSA 泛洪扩散到其邻接的路由器上，再由邻接路由器向它们的其他接口泛洪扩散该 LSA 直到整个网络。

1. 工作流程图

下图将以两台路由器为例，介绍在以太网模型中，两台路由器的从失效状态到完全邻接状态的详细步骤以及该过程中涉及的相关报文种类。

说明：为了描述方便，图示中 LSA 同步在 DD 交换之后才进行，而在实际工作流程中这两个步骤是交替进行的。

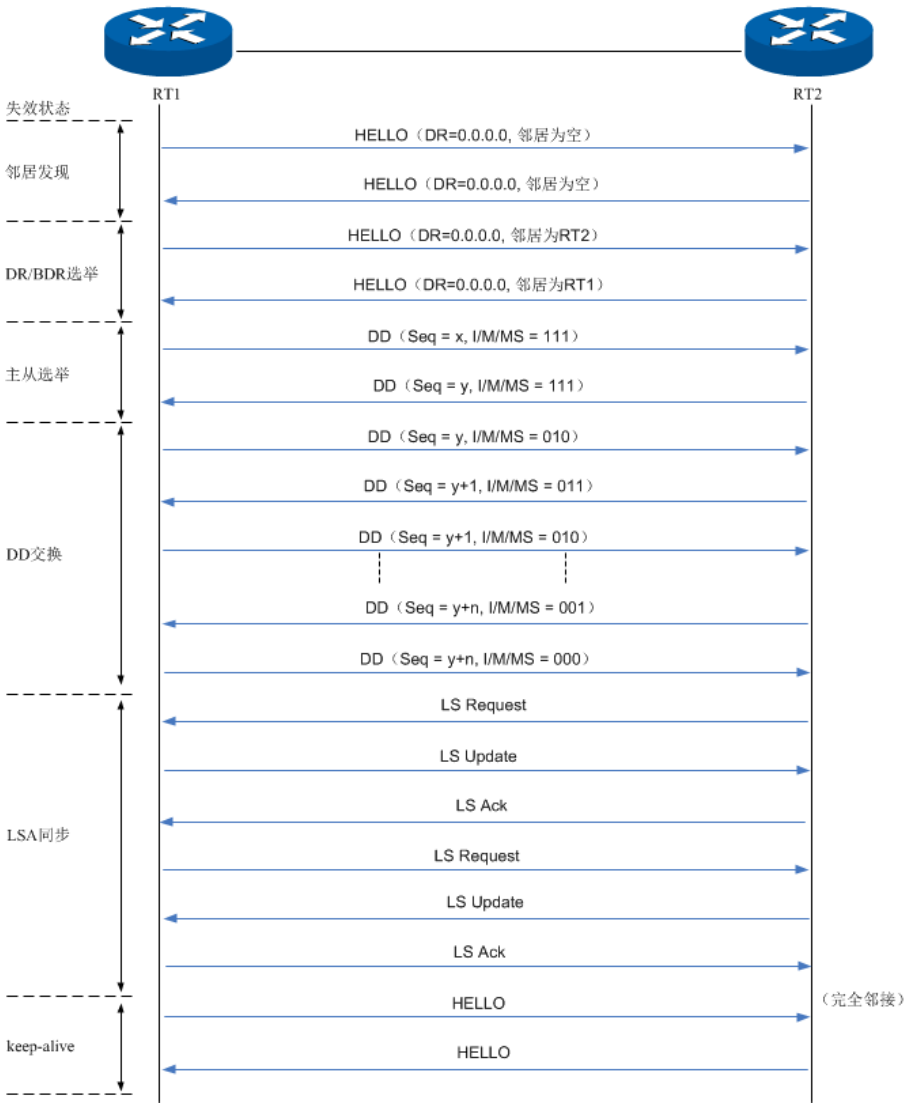


图 10-31 完全邻接步骤

路由器建立邻接关系的过程中，所有的接口参数均会影响到这个过程，例如路由器 ID 的大小、接口所属的区域 ID、接口优先级和路由器优先级等等。请先进行完整的网络规划后再配置各类参数，后续章节将统一介绍相关参数。

2. 泛洪扩散

如图 10-31 所示，在任意两台路由器通过 LSA 请求、LSA 更新和 LSA 确认报文来同步链路状态数据库。但在实际的路由网络模型中，路由器又是如何将本地网络的变更通过 LSA 更新报文泛洪扩散到整个网络的呢， 图 10-32 详细介绍在广播型网络中 LSA 更新报文的泛洪过程。

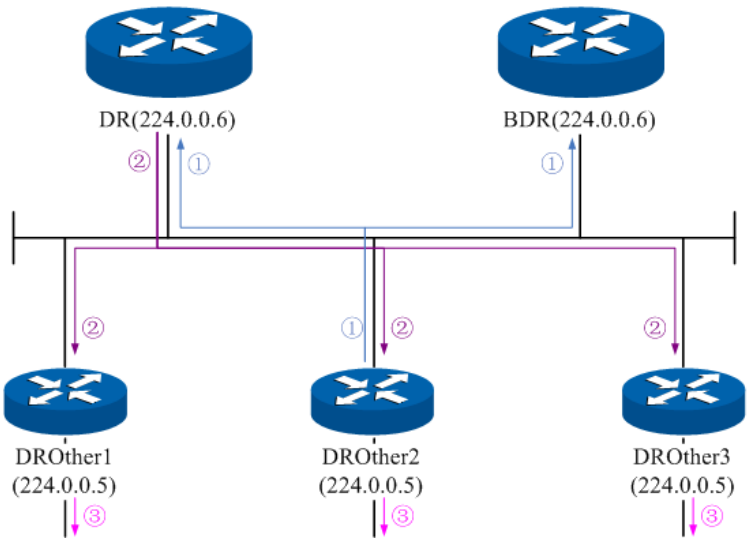


图 10-32 LSA 泛洪扩散

1) DROthers 向 DR 和 BDR 以组播形式发出自己直连网络中的 LSA 更新。

2) DR 路由器收到 LSA 更新后，向所有与之有邻接关系的邻居路由器泛洪该 LSA 更新。

3) 邻居路由器收到 DR 的 LSA 更新后，在它们同区域下的其他 OSPF 接口泛洪该 LSA 更新。

- **区域和路由聚合**

OSPF 协议通过邻接关系使网络中的每台路由器均能够获得完整的网络拓扑，并以此计算路由表和完成网络数据的转发。随着网络规模日益扩大，每台路由器需要消耗大量的资源来存储 LSDB 和计算路由表，而网络拓扑结构的小变化也会使全网络的路由器全部重新同步和计算，使网络经常处于“振荡”之中。

为了使 OSPF 协议在大型网络中能够有效工作，可以通过区域划分将一个自治系统中的路由器从逻辑上划分区域，用 Area ID 来标识。划分区域后，位于区域内部的路由器按照标准的 OSPF 路由协议完成路由寻址和转发数据；位于多个区域边界的路由器则需要将各区域的路由信息聚合后汇总给骨干区域，标识为区域 0，再由骨干区域将这些汇总信息通告给其他区域。下图为区域划分模型。

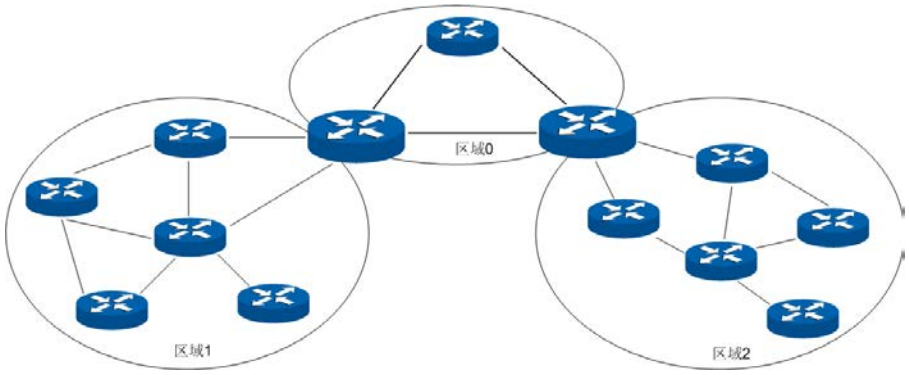


图 10-33 区域模型

如图所示，一个大型网络中被划分为三个区域，区域 1 和区域 2 通过两台边界路由器将路由信息通过骨干区域 0 发布给对方区域。骨干区域 0 必须时刻保持自身网络的连通。对于非骨干区域 1 和区域 2，相互之间不能直接通信，必须通过骨干区域 0 来转发路由信息。在大型网络中合理划分区域能够极大的节约网络资源，同时提高路由选路速度。

划分区域后，网络中的路由器因位置不同则需要完成不同的工作，而不同区域因和骨干区域的相对位置不一样则需要不同的方式将路由信息传递到骨干区域，接下来将详细介绍划分区域后相关细节。

1. 路由器类型

如图 10-34 所示，网络中划分区域后，路由器因分属于不同区域的位置而需要完成不同的工作，根据路由器的位置可以将路由器分为四类，区域内路由器 IR、骨干路由器 BR、区域边界路由器 ABR 和自治系统边界路由器 ASBR。

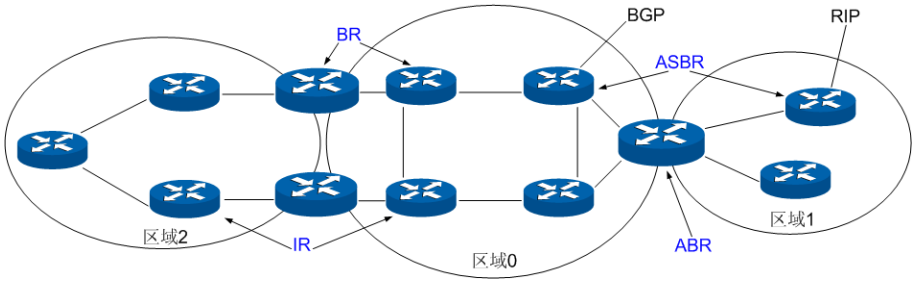


图 10-34 路由器分类

表 10-1 为不同类型路由器的职责划分：

路由名称	特点	职责
IR	所有路由接口属于同一个区域的路由器	将自身的所有链路和接口信息与同区域的邻接路由器进行泛洪交换，使区域内路由器拥有相同的链路状态数据库。
BR	至少有一个路由接口属于骨干区域	通过 ABR 将同一自治系统中所有区域的路由拓扑信息进行汇总，为各区域转发通信数据。
ABR	连接一个或多个区域到骨干区域的路由器	为不同区域维护独立的链路状态数据库，将各区域的拓扑信息以自己的中间路由节点通过骨干区域传递给其他区域。
ASBR	通过其他路由协议与 OSPF 自治系统外的路由器相连	为不同路由协议维护独立的路由表，可以将其他路由选择协议学习到的路由信息通过一定的标准注入到 OSPF 域，形成统一的路由表。

表 10-1 路由器类型

2. 虚链路

在实际应用中，可能会因为物理条件限制导致部分区域的 ABR 并没有直接连接到骨干区域，这时可以通过配置 OSPF 虚链路（Virtual Link）予以解决。虚链路示意图如下图所示。

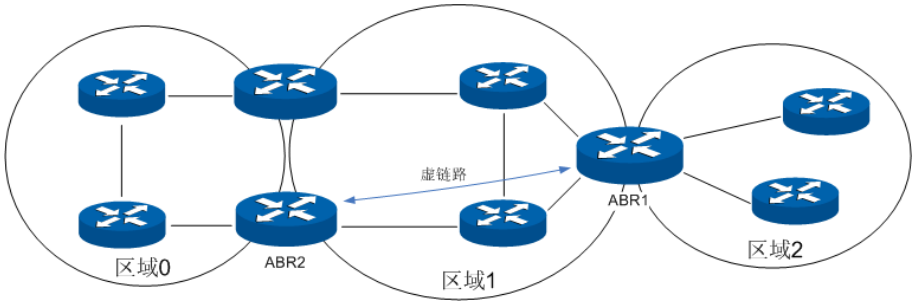


图 10-35 虚链路示意图

如图 10-35 所示，区域 2 的 ABR 没有与骨干区域直接连接的物理链路，在不设置虚链路的情况下，区域 2 将无法与外界进行通信。此时如果在 ABR1 和 ABR2 之间建立一条穿越区域 1 的虚链路，这条虚链路为区域 2 提供了一条与骨干区域连通的逻辑链路。

虚链路相当于在两个 ABR 之间设置了一个点到点的连接，因此，在虚链路两端的两个路由器接口只需在普通路由接口的基础上配置简单的虚链路参数即可。两台 ABR 之间相互以对方接口 IP 为目的地址直接交换 OSPF 报文，它们之间的 OSPF 路由器将这些报文作为普通的 IP 报文来转发。

虚链路通常作为一种临时手段用来修复网络拓扑问题，其存在往往会增加网络的复杂度，因此在实际组网过程中需要尽量避免使用虚链路。

3. stub 区域和 NSSA 区域

stub 区域即末梢区域，当一个区域仅通过 ABR 连接到自治系统内，目的为区域外的通信数据只能通过 ABR 往外转发，此时我们可以将此区域设置为 stub 区域。将某个区域配置为 stub 区域后，ABR 不再将 AS-External LSA 描述的外部路由信息向区域内泛洪，同时生成一条目标网络为 0.0.0.0 的默认路由，并发布给本区域中的其他路由器，使得所有发往外部路由均发往 ABR，通过 ABR 向外转发数据。由于无需了解其他区域的路由信息，stub 区域内路由器的路由表规模以及路由信息传递的数量都会大大减少。

NSSA（Not-So-Stubby Area）区域与 stub 区域类似，与 stub 区域有许多相似点，不过它不是纯末梢区域。NSSA 区域也不允许 ABR 将 AS-External LSA 描述的外部路由信息注入，但允许区域中的 ASBR 将其他路由协议学习的路由信息以 Type-7 LSA 在 NSSA 区域内传播，当区域中的 ABR 收到其他路由协议学习的路由信息时，可以将此类路由信息转换为 Type-5 LSA 泛洪扩散至整个 AS 系统。

4. 路由聚合

路由聚合是指将具有相同前缀的路由信息聚合，只发布一条聚合路由。合理配置路由聚合将大大缩减 LSDB 的大小。

ABR 路由聚合：当网络规模较大时，在 ABR 上配置路由聚合，可以将单区域内的网络地址信息聚合成范围更广的地址信息，减少通报到其他区域的路由条目。如图 10-36 所示，ABR1 可以在区域 1 中配置聚合路由 192.161.0.0/16 并向骨干区域发布，而 ABR2 则可以在区域 2 中配置聚合路由 192.162.0.0/16 并向骨干区域发布。

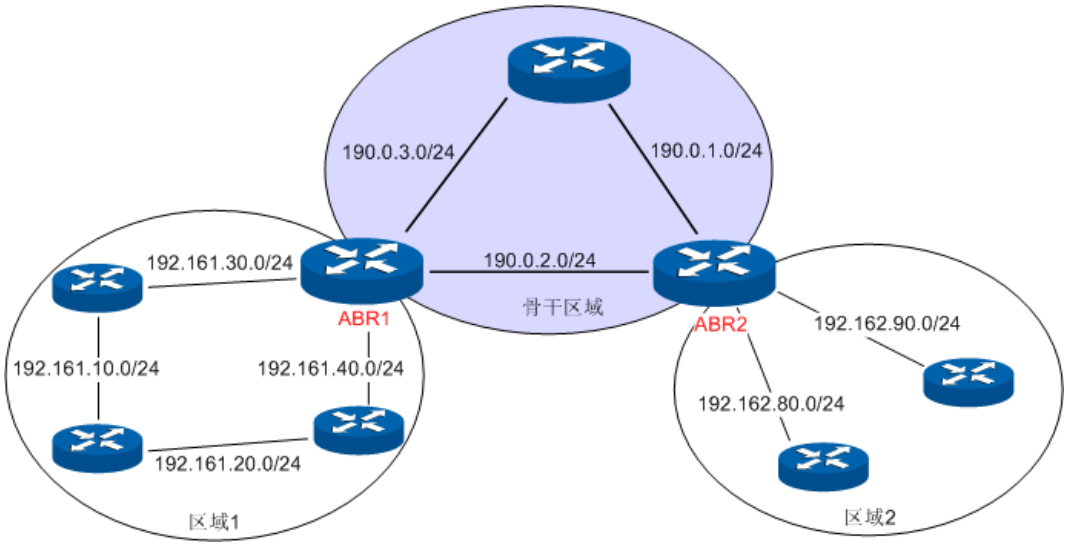


图 10-36 ABR 路由聚合

需要注意的是，如果网络规划为不连续子网模式，那么配置路由聚合时则需要小心配置，否则有可能出现某些网络不可达的情况。如图 10-37 所示，如果仍然按照上述方法在 ABR1 和 ABR2 上配置路由聚合，则有可能出现路由不可达的情况。在这种情况下，建议只在一台 ABR 上都配置路由聚合。

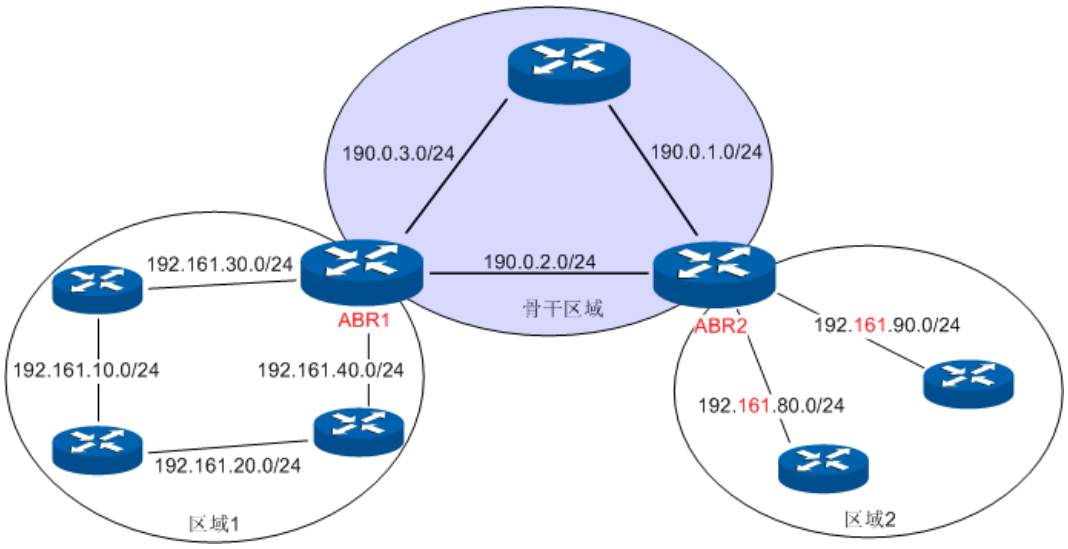


图 10-37 不连续子网划分

ASBR 路由聚合：如果在 ASBR 上配置了路由聚合，它将对引入聚合地址范围内的 AS-External LSA 进行聚合。当配置了 NSSA 区域时，还要对引入聚合地址范围内的 Type-7 LSA 进行聚合。ASBR 路由聚合的配置原理与 ABR 路由聚合类似，只不过聚合的对象是外部路由。

- **链路状态数据库**

当网络中的路由器通过交换 LSA 达到链路状态数据库完全同步时，就可以利用链路状态数据库以自己为根节点计算最短路径树。OSPF 协议路由的计算过程可简单描述如下：

1) 每台 OSPF 路由器根据自己的链路连接情况或路由信息生成 LSA（Link State Advertisement，链路状态通告），并通过更新报文将 LSA 发送给网络中的其它 OSPF 路由器。LSA 是对网络拓扑结构和路由信息的描述，如 Router-LSA 描述路由器链路连接情况，Summary-LSA 描述区域间汇总路由等。

2) 每台 OSPF 路由器将收集到的其它路由器通告的 LSA，放在一起组成 LSDB（Link State Database，链路状态数据库）。LSDB 中的所有 Router-LSA 和 Network-LSA 是对整个区域内网络拓扑结构的描述，其他类型的 LSA 描述了到达某目的地的路由。

3) 当网络中所有路由器的 LSDB 完全同步时，每一台 OSPF 路由器将使用 SPF 算法来计算一个无环路的拓扑图，以描述它所知道的到达网络中每一个目的地的最短路径，这张拓扑图就是 SPF 算法树。

4) 每台路由器根据 SPF 算法树构建出自己的路由表。

- **OSPF 协议报文类型**

OSPF 路由协议在整个路由学习过程中使用了五种报文，均为 IP 报文，IP 头部的协议字段为 89 表示该报文为 OSPF 报文。本设备遵循标准的 RFC 协议，接下来将介绍 RFC 文档中定义的 OSPF 路由协议运行过程中涉及的报文格式，同时提供报文格式图片及主要字段的意义。

1. OSPF 首部

OSPF 路由学习过程中使用了五种报文，具有共同的 OSPF 首部，如下图所示。

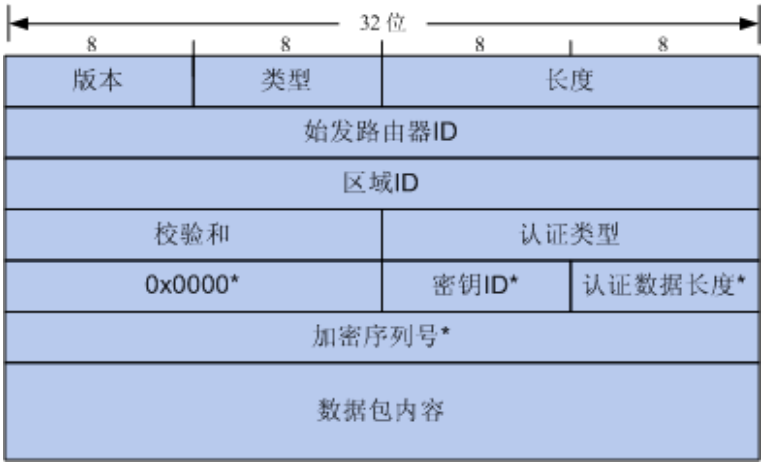


图 10-38 OSPF 首部

1) 版本：指示本设备运行的 OSPF 版本号，在我司 IPv4 设备中运行为 OSPFv2 版本，IPv6 设备中运行为 OSPFv3 版本。

2) 类型：指示该报文的类型，共有五种 OSPF 报文类型，如下表所示。

类型代码	报文名称
1	HELLO 报文
2	数据库描述报文（DD）
3	链路状态请求报文（LSR）
4	链路状态更新报文（LSU）
5	链路状态确认报文（LSAck）

表 10-2 OSPF 报文类型

3) 始发路由器 ID：指示发出该报文的路由器 ID。

4) 区域 ID：指示发出该报文的路由接口所属区域 ID。

5) 认证类型：指示该报文使用的认证模式，在该字段后方的打*号的字段均为认证的必要信息，如下表所示。

类型代码	认证名称	认证特点
0	无需认证	其后 64 位认证信息字段均为 0。
1	简单口令认证	后面的 64 位认证信息将作为口令进行认证。
2	MD5 密文认证	由密钥 ID、认证数据长度和加密序列号共同进行 MD5 密文认证。

表 10-3 认证类型

2. HELLO 报文

OSPF 路由器相互发送 HELLO 报文来发现网络中的邻居路由器，并维护相互之间的邻接关系。只有 HELLO 报文中携带的接口相关参数一致，两台路由器之间才能成为邻居。

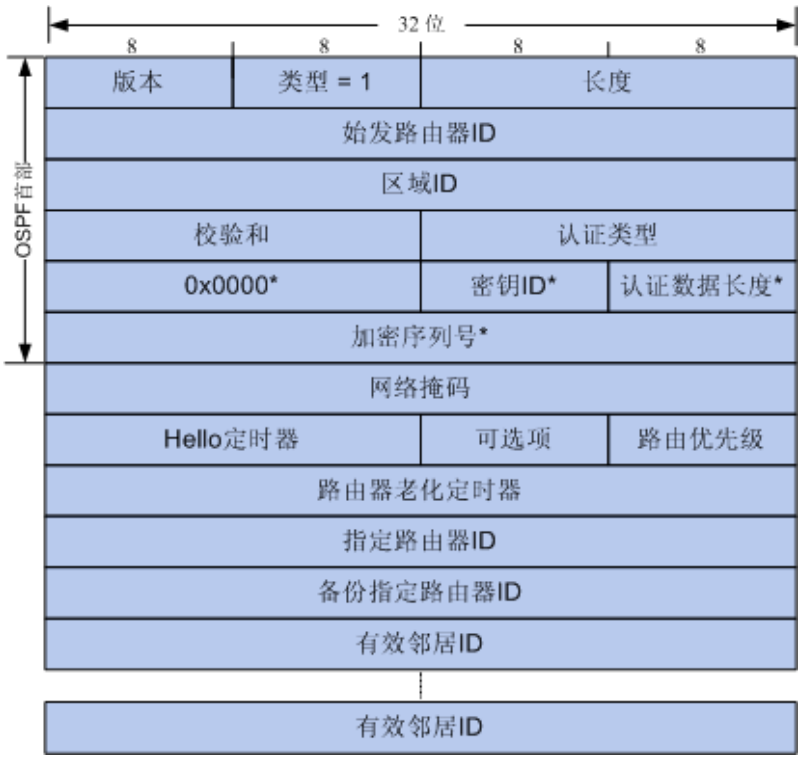


图 10-39 HELLO 报文

1) 网络掩码：指示发出该 HELLO 报文的路由接口的网络掩码。只有发送接口和接收接口的网络掩码一致时，两台路由器才能相互成为邻居。

2) Hello 间隔：指示发送接口连续发出的 HELLO 报文之间的时间间隔。只有 Hello 间隔一致的路由器才能相互成为邻居

3) 路由器优先级：该字段决定了该网段中 DR/BDR 的选举结果。当始发路由器的优先级值最大时表示拥有最高优先级同时将可能选举为该网段的 DR；当优先级值为 0 时，表示始发路由器不具备选举权。

4) 路由器老化间隔：接收路由器在指定老化时间内如果没有收到始发路由器另一个 HELLO 报文更新，则将始发路由器在其邻居列表中老化删除。只有老化间隔时间一致的路由器才能相互成为邻居。

5) 指定路由器 ID：指示在始发接口网络中，始发路由器认定的指定路由器的接口 IP。

6) 备份指定路由器 ID：指示在始发接口网络中，始发路由器认定的备份指定路由器的接口 IP。

7) 邻居：指示始发路由器的所有邻居列表，此处列出的是各接口网段的邻居接口 IP 地址。

3. DD 报文

两台路由器成为邻居后，相互之间将自身链路状态数据库中的所有路由信息（即 LSA）的首部，通过 DD 报文发送出去，接收路由器以此进行数据库同步。

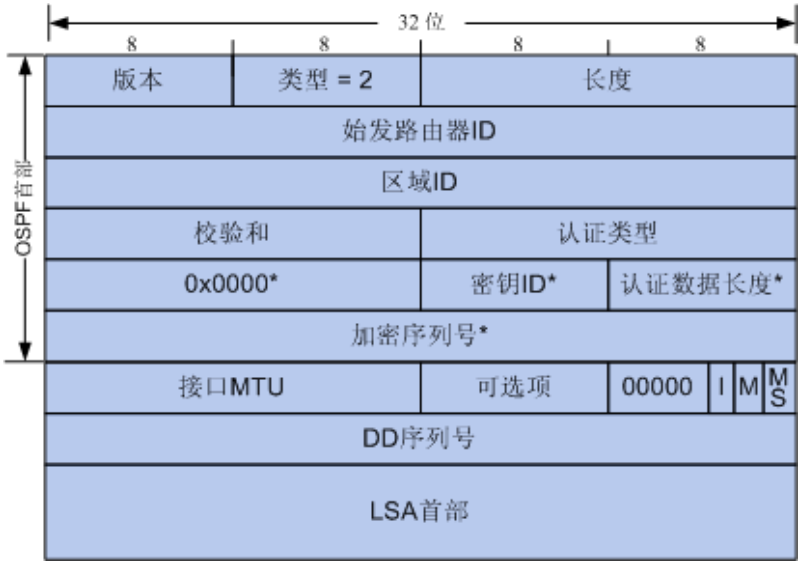


图 10-40 DD 报文

1) 接口 MTU：指示始发路由器的路由接口所能发送的最大 IP 报文的长度。

2) I：初始位标志。两台路由器同步数据库过程中可能需要相互发送多个 DD 报文，路由器发出的第一个 DD 报文时，I 位将置为 1，其余时刻 I 位为 0。

3) M：后继位标志。当已发出的 DD 报文不是最后一个数据库时，该位置为 1，最后一个 DD 报文的 M 位置为 0。

4) MS 位：主从位。两台路由器开始同步数据库之前需要进行主/从路由器选举，通常由路由器优先级、路由器 ID 等参数决定，选举成功后，由主路由器主导数据库同步过程。主路由器发出的 DD 报文 MS 位置为 1，从路由器发出的 DD 报文 MS 位置为 0。

5) DD 序列号：主/从路由器选举后，由主路由器随机确定第一个 DD 报文的序列号，后续的 DD 报文序列号依次加 1，从而保证整个同步过程能够有序进行。

6) LSA 首部：始发路由器的链路状态数据库中部分或全部的 LSA 首部，其唯一标识了一个 LSA。

4. LSR 报文

两台路由器同步链路状态数据库的过程中，如果在对方发出的 DD 报文内发现自己没有或更新的 LSA，即可通过发送 LSR 报文请求完整的 LSA 内容。

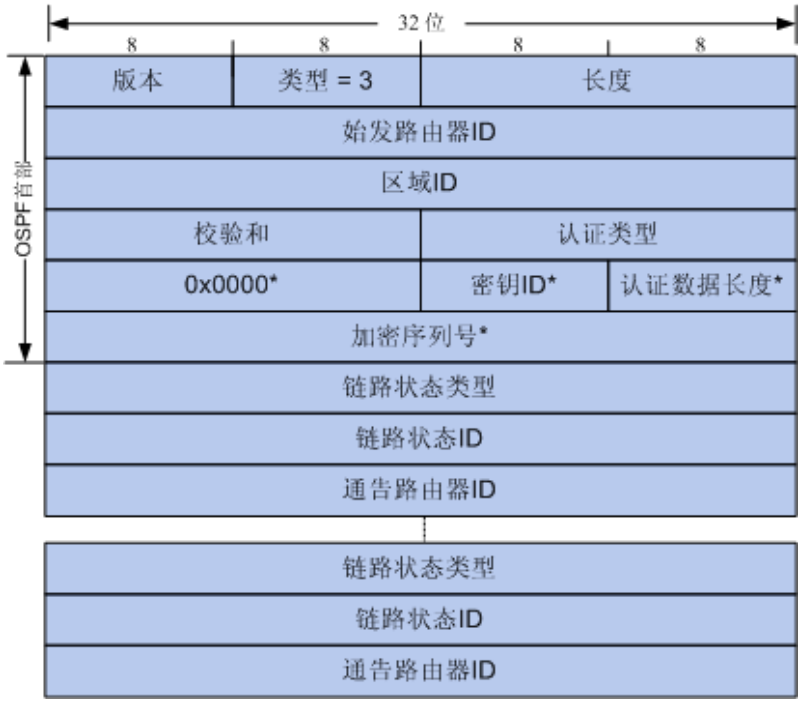


图 10-41 LSR 报文

1) 链路状态类型： 指明该 LSA 的类型，共有 11 种 LSA 类型，包括路由器 LSA、网络 LSA、网络汇总 LSA、ASBR 汇总 LSA 等等，后续将详细介绍 LSA。

2) 链路状态 ID：不同的 LSA 该字段的意义也不同，路由器 LSA 的链路状态 ID 表示始发路由器的 ID，网络 LSA 的链路状态 ID 表示 DR 的接口 IP 地址，网络汇总 LSA 表示其通告的网络或子网的 IP 地址，此处将不详细列举。

3) 通告路由器：指明始发该 LSA 的通告路由器的路由器 ID。

5. LSU 报文

当路由器收到 LSR 时，将发出 LSU 报文告知对方完整的 LSA 信息；收到 LSA 更新的路由器将重新封装该 LSA 并泛洪扩散。

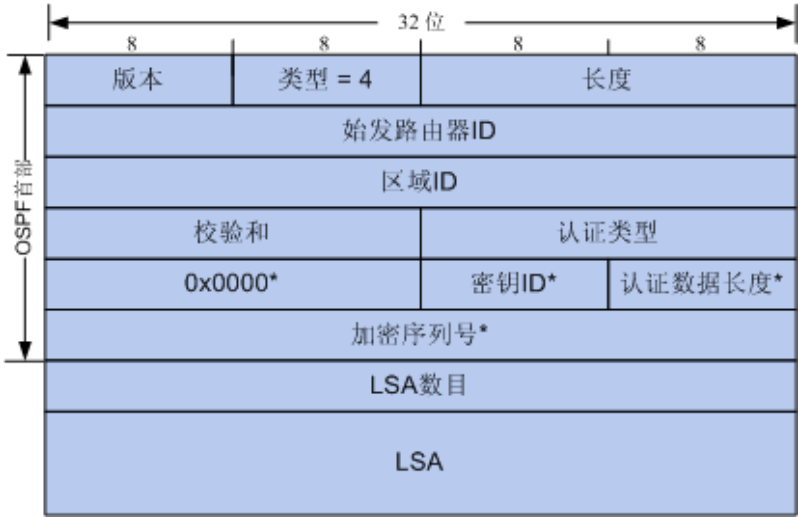


图 10-42 LSU 报文

1) LSA 数量： 指示该 LSU 中包含的 LSA 的数量。

2) LSA：此处完整的描述 LSA。

6. LSAck 报文

当路由器收到 LSU 时，将向始发 LSU 报文的路由器发出 LSAck 报文，报文中包含自己收到的 LSA 的首部，确认自己收到的数据是否正确。

7. LSA

OSPF 协议定义了区域和多种路由器类型，不同的路由器通过各种类型的 LSA 来完成网络变化引起的路由更新。OSPF 协议定义了 11 种 LSA 类型，所有的 LSA 均具有相同的 LSA 首部，如下图所示，每一个 LSA 在网络中都是唯一的，均能够通过 LSA 首部中的主要字段进行唯一标识。

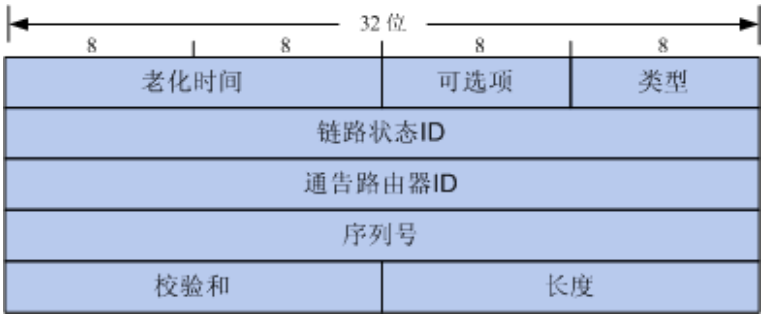


图 10-43 LSA 首部

1) 老化时间： 指示该 LSA 产生后所经过的时间，当老化时间超过路由器系统设置的老化时间阈值（1h）且没有收到该 LSA 的更新时，将删除相应的 LSA。

2) 类型：指示该 LSA 的类型，表 10-4 中列举了常用的几种 LSA 特征。

3) 链路状态 ID：根据不同的 LSA 类型，该字段具有不同的意义，详细描述请参考 RFC2328 文档。

4) 通告路由器 ID：指明通告该 LSA 的始发路由器的 ID。

5) 序列号：指示某个 LSA 的唯一性，当 LSA 内容有更新时，将通过序列号加 1 并泛洪到网络中。

常见的 LSA 类型有如下六种，下表为六种常见 LSA 的特征。

类型代码	名称	特点
1	路由器 LSA	始发于所有路由器，描述自身已启用 OSPF 特性的路由接口，在其始发的区域内传播。
2	网络 LSA	始发于 DR，描述其连接的网段中所有路由器的链路状态，在其始发的区域内传播。
3	网络汇总 LSA	始发于 ABR，描述区域内各网段的路由，并通告给骨干区域，由骨干区域路由重新汇总后通告到其他区域。
4	ASBR 汇总 LSA	始发于 ABR，描述从 ABR 到 ASBR 的路由，将到达 ASBR 的路径通告给 ABR 所连接的区域。
5	AS 外部 LSA	始发于 ASBR，描述 ASBR 通过其他路由协议获得的外部路由以及可到达的网络，该类型 LSA 将泛洪到整个 AS 系统。
7	NSSA 外部 LSA	始发于 NSSA 区域的 ASBR，该 LSA 内容同 AS 外部 LSA，只是该 LSA 仅通告到 NSSA 区域，ABR 可以将此类路由信息转换为 AS 外部 LSA 后，扩散至整个 AS 系统。

表 10-4 LSA 类型

➢ **交换机支持的 OSPF 特性**

本交换机支持标准的 OSPF 路由特性，适用于各种网络环境中，能够满足以太网中场景的常见的组网需求。以下是我司交换机支持的 OSPF 特性。

1) 支持多进程。我司交换机上可以建立多个路由进程，每个进程相互独立，拥有独立的数据库，每个路由接口只能属于固定的进程。简而言之，在一台交换机上建立了多个进程就相当于将一台交换机在逻辑上划分出多台独立的交换机。

2) 支持区域划分。能够将一个自治系统按照用户指定的原则进行区域划分，同一区域中的路由器只需要和本区域中的路由器同步 LSA，降低了区域内路由器的性能要求从而降低组网成本。

3) 支持配置多条等价路由进行负载均衡和线路备份。

4) 支持路由重发布。OSPF 可以注入其它路由协议学习到的路由信息，不同 OSPF 进程学习到的路由信息也可以相互注入。

5) 在同一区域的邻居路由器报文交互时，支持简单密码认证和 MD5 认证，提高安全性。

6) 支持多项接口参数的自定义配置，包括接口开销、路由信息重传时间间隔、接口传输延迟、路由优先级、路由老化时间、hello 信息时间间隔和认证密钥等，能够灵活适应多种网络需求。

7) 支持虚链路配置，在网络划分多个区域时，能够将物理位置较远的区域通过虚连接的方式直接连接到骨干网络。

8) 支持 Stub 区域和 NSSA 区域配置。

9) 支持 ABR 路由聚合，能够将具有相同前缀的区域内路由信息聚合，只发布一条路由到其他区域。

10) 支持 ASBR 路由聚合，能够将具有相同前缀的外部路由信息聚合，只发布一条路由到整个自治系统。

➢ **配置简介**

OSPF 协议中定义了多种参数来保证 OSPF 路由协议工作过程的有序进行，配置 OSPF 路由协议时，需要统一规划自治系统中的所有路由器的配置参数。这种规划造成了 OSPF 路由协议的配置在一定程度上的复杂度。然而在实际使用过程中，大多数参数只是在特殊需求的情况下才需要配置，简而言之，大多数参数可以保留为缺省值，只进行基本的配置工作即可。配置 OSPF 路由协议包括如下五个必要步骤。

1) 使能交换机上的路由特性。默认情况下，路由特性已使能，无需额外操作。

2) 创建路由接口，并配置网络 IP 地址。

3) 规划确定交换机上各子网所属于的区域，即路由接口所属的区域。

4) 配置每台交换机上的 OSPF 进程。

5) 配置 OSPF 进程下包含的路由接口以及它们所属的区域。

如上操作后，交换机上的 OSPF 路由协议即可正常工作。如网络拓扑比较特殊，也可以根据实际需求参考 WEB 详细介绍来优化配置参数。

10.9.1 进程配置

在进程页面中可以创建 OSPF 协议进程。不同 OSPF 进程独立运行，互不影响，需要通过路由重发布才能相互通告路由。路由器的一个接口只能属于某一个 OSPF 进程。需要注意的是，进程只对于本地设备有效，在常见网络应用中，一台路由器上建立一个进程即可。如果因组网需要，可以在路由器上建立多进程实现网络隔离，并进一步通过路由重发布进行路由备份。

进入页面的方法： **路由功能>>OSPF>>进程配置**

图 10-44 进程配置

条目介绍:

- **OSPF 进程配置**

进程 ID: 输入 1-65535 之间任意整数作为进程号。

路由器 ID: 设置路由器 ID，在一个自治系统中标识自己的唯一性。路由器 ID 是一个 32 比特无符号整数，格式为点分十进制。路由器 ID 可以手动配置，也可以由路由器自动选举。为避免自动选举时多台路由器使用相同的路由器 ID，建议手动配置此项。

- **OSPF 进程列表**

选择: 勾选进程进行配置。

进程 ID: 显示进程 ID。

活跃的路由器 ID: 显示对应的 OSPF 进程下路由器使用的 ID。

路由器 ID: 输入路由器 ID 参数对路由器 ID 重新定义，点击**提交**后生效。

状态: 显示进程状态。

- Running：显示该进程当前正常运行。
- Pending: 该进程没有设置路由器 ID 因此无法启动，如需要启动该进程，请设置路由器 ID。

重启： 重新启动勾选的进程。重新配置了路由器 ID 后，建议重新启动进程，让路由器以新的身份 ID 重新开始对外交互路由信息。

10.9.2 基本配置

在本页面中，可以设置 OSPF 协议进程的全局路由参数。

进入页面的方法： **路由功能>>OSPF>>基本配置**

图 10-45 基本配置

条目介绍:

- **选择当前进程**

当前进程: 从下拉列表中选择需要配置的进程，勾选后此页面下方进行配置保存时只对相应的进程生效，或者显示该进程的部分特征参数。

- **配置发布默认路由**

发布: 使能 Originate 特性。使能 Originate 特性后，路由器以 AS-External-LSA 向自治系统通告目标网络为 0.0.0.0 的默认路由。

Always: 使能 Originate 特性后，如果 Always 选项为 DISABLE，路由器只会在路由表中包含默认路由表 0.0.0.0 时广播该默认路由；如果设置 Always 选项为 ENABLE，则无论路由器是否有默认路由 0.0.0.0，均广播默认路由。推荐将 Always 选项设置为 ENABLE，并手动添加默认路由条目。

度量值: 设置发布默认路由时的度量值，默认值为 1。

度量值类型: 设置发布默认路由时的度量值类型，External Type 1 表示接收路由器在记录默认路由时将度量值设为上面的 Metric 值加上自身到达本路由器的度量值，而 External Type 2 表示接收路由器在记录默认路由时将度量值设为上面的 Metric 值。

- **OSPF 配置**

ASBR 模式: 显示该进程的 ASBR 角色特征。如果该进程下配置了路由重发布或默认路由广播，则认为该路由器是一台 ASBR。

ABR 状态: 显示路由器的 ABR 角色特征。如果路由器上设置了多个区域，且每个区域有活跃的非虚链路接口，则认为该路由器是一台 ABR。

管理距离: 配置 OSPF 进程的路由距离。当多个 OSPF 进程或多种路由协议含有指向相同目的路由条目时，只有路由距离最短的路由条目会被添加到 IP 路由表。路由距离的出厂默认值为 110。

RFC1583 兼容: 选择 RFC1583 兼容性，该参数影响路由器在收到具有相同目标的 AS-external LSAs 时的处理规则。我司路由器 OSPF 协议按照 RFC2328 实现的，在与 RFC1583 实现的路由器混合组网时，由于算法差异，可能会出现路由环路。在整个 OSPF 路由域中，该参数必须一致，以减少可能出现的路由环路。

SPF 延迟: 设置 SPF 延迟时间，该时间为路由器收到 LSA 路由更新信息时将延迟设定的时间段后，才重新计算 SPF 路由，以避免实时计算 SPF 路由导致的因路由过度更新而产生大量的路由计算，保护路由资源。SPF 的出厂默认值为 5s。

SPF 间隔: 设置两次 SPF 路由计算之间的时间间隔，该时间值如果设置过短可能会导致因路由计算频繁而消耗路由器资源，设置过长可能会导致路由更新不及时，在网络拓扑发生变化时出现短时间的转发错误，如无需要请保持出厂默认值 5s，并关注网络情况进行调整。

外部 LSA 总数: 显示路由器的链路状态数据库中包含的外部 LSA 数量。

外部 LSA 校验和: 链路状态数据库中所有 AS-External LSA 的校验总和。

始发 LSA 数量: 显示路由器始发的 LSA 数量。

接收的 LSA 数量: 显示路由器收到的 LSA 数量。

默认度量值: 配置重发布路由的度量值，该参数指相应进程在收到其他进程或路由协议发布的路由信息时，将度量值固定为设定值，出厂默认值为 20。在**路由重发布**页面中设置该进程的路由重发布时，如果将度量参数留空不设置则此处的度量值参数将生效，且具体的度量值同时被度量值类型影响。

最大路径数: 配置路由器可以保存的到达同一目的的路径数量，默认为 5 个。

默认被动模式: 配置该进程的全局被动模式，该参数对相应进程下的所有接口生效。使能该项后，接口层面的被动模式会被覆盖，相应进程下的接口将不再与其他路由器建立邻接关系，仅对外发布 LSA 标明直连网络。

自动开销/参考带宽:	配置接口自动计算链路开销。使能了自动计算开销参数后，除非手动设置接口开销，否则路由的接口开销将自动以计算公式为10^8/基础带宽进行计算。禁用自动计算开销参数后，路由学习时只能手动设置接口开销或使用缺省值。

10.9.3 网络配置

在本页面中，可以设置区域包含的网段，连接到该网段的接口将与相应的区域关联。

进入页面的方法： **路由功能>>OSPF>>网络配置**

图 10-46 网络配置

条目介绍:

- **网络配置**

进程 ID:	选择需要配置的进程，配置参数只对相应的进程生效。
IP 地址/通配符掩码:	输入网段的 IP 地址及通配符掩码。通配符掩码规则为用目标 IP 地址与通配符掩码进行匹配，位 0 表示严格匹配，位 1 表示无需匹配，如果匹配结果与此处设置的 IP 地址相同，则认为目标 IP 为范围内的 IP。**通配符掩码**也可以输入子网掩码格式，交换机能够自动识别并转换。
区域 ID:	输入区域 ID，区域 ID 为无符号整数，长度为 32bit，可以用十进制或点分十进制，匹配了 **IP 地址/通配符掩码**参数的接口将认为与相应区域关联。如果**区域配置**页面没有创建相应的区域，交换机将同时使用区域默认参数创建一个新的区域。

- **网络列表**

在网络列表区，可以查看所有 OSPF 进程中已存在的网络，并可以删除多余的网络。

10.9.4 接口配置

在本页面中，可以查看当前交换机上创建的接口，并根据接口直连的网络、对端设备特征配置接口参数。

进入页面的方法： **路由功能>>OSPF>>接口配置**

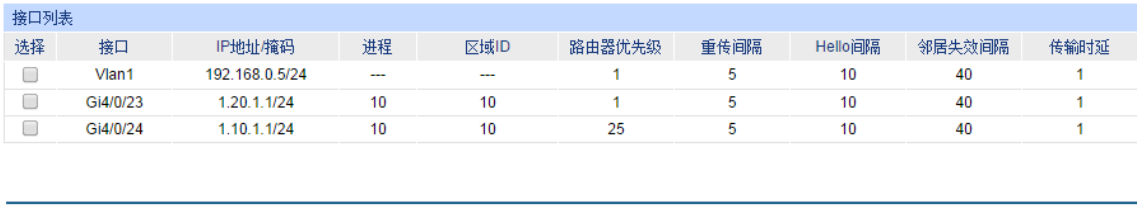


图 10-47 接口配置

在接口列表中，可以查看当前所有接口 OSPF 配置信息。选择接口进行配置，可以同时选择多个接口，请参考如下图示配置，只有重新输入参数的配置项会修改参数，留空的配置项表示保持当前参数值不变。

图 10-48 修改接口参数

条目介绍:

接口: 显示当前配置的接口列表。

路由器优先级: 配置接口的路由器优先级，优先级范围为 0-255，0 表示路由器在相应的接口网络中不能被选为指定路由器，数值越大表示优先级越高。出厂默认值为 1。建议将硬件较为健壮的路由器设为中心路由器，并将优先级设置调高。

重传间隔: 接口的重传间隔，单位秒，用于邻接之间重传 LSA 和 DD 报文。合法范围是从 1 到 65535，默认值为 5。

Hello 间隔: 配置接口发送 hello 报文的时间间隔。在同一网络上，只有 Hello 间隔一致的接口才能形成邻接关系，请务必保证所有接口的 Hello 间隔保持一致。出厂默认值为 10 秒。

邻居失效间隔： 配置路由器宣告邻居失效的时间间隔。在指定时间内，如果没有收到邻居的 Hello 报文，则认为该邻居失效。出厂默认值为 40 秒。

传输时延： 在接口上传输链路状态更新报文需要的时间，默认为 1 秒。

开销： 配置接口路径开销。OSPF 基于接口开销值计算从该接口进行路由转发数据的最短路径。如果不手动配置，将由 OSPF 自动计算接口路径开销，如果自动计算开销特性没有使能，则使用默认值作为接口路径开销。默认值为 1。

网络类型： 配置接口的网络类型，以太网的默认网络类型是 broadcast，除非确有必要，否则不建议修改。

被动模式： 配置接口的被动模式，配置为被动模式后，相应接口不与其他路由器建立邻接关系，该路由器连接 OSPF 会以末梢网络的方式在 router-LSA 中发布被动接口直连的网络。默认情况下，接口没有开启被动模式。

忽略 MTU 检查： 启用后，接口收到数据库描述报文时会忽略 MTU 字段匹配检查。默认未启用该特性，接口会对数据库描述报文进行 MTU 长度匹配检查，如果 DD 报文中的 MTU 字段不匹配，则无法完成 DD 交换。

数据库过滤： 配置接口是否泛洪 LSA。默认禁用，所有合法 LSA 均可以从接口泛洪出去，其他路由器能够通过该接口获得该路由器上的 LSA 信息。

认证类型： 配置接口的认证类型，只有认证类型及密码一致的接口才能形成邻接关系并同步 LSA，包含以下认证方式：

default：接口使用所属区域的认证方式。

null：不认证。

simple：简单密码认证。

md5：md5 加密认证。

简单密码： 输入用于简单认证的密码。

MD5 密码 ID： 输入用于 md5 加密认证的密码 ID。

MD5 密码： 输入用于 md5 加密认证的密码。

10.9.5 区域配置

在本页面中，可以根据当前网络划分以及路由器的网络位置创建区域，并设置区域属性。合理划分区域后可以减少网络中 LSA 的数量。

进入页面的方法： **路由功能>>OSPF>>区域配置**

图 10-49 区域配置

条目介绍:

- **区域配置**

进程 ID: 选择进程，创建的区域将属于相应进程。

区域 ID： 配置区域 ID。区域 ID 是一个 32 比特无符号整数，格式为十进制或点分十进制。

区域描述： 配置区域描述信息，通常可以以区域覆盖的网络的物理属性进行描述，以便于区分各个区域。

认证类型： 配置该区域中进行 OSPF 报文交互时使用的认证类型，相同区域的路由接口认证类型必须保持一致，同一网段中只有认证类型保持一致的路由接口才能形成邻接关系。为了提高网络安全性，建议设置为 MD5 认证。

null：不认证。

simple：简单密码认证。

md5：使用 md5 加密认证。

默认开销： 发布默认 Summary-LSA 时的度量值。合法范围是从 1 到 16777214。

汇总： 配置交换机是否允许将其它区域的 Summary LSA（网络汇总 LSA）向本区域发送，默认启用。在 Normal 区域中总是启用，不能设置为禁用。

重发布： 配置交换机是否允许将外部路由发布到本区域。在 Normal 区域总是启用该特性，在 Stub 区域总是禁用。

发布默认路由： 配置交换机是否允许通过 NSSA-External LSA 发布默认路由 0.0.0.0 到 NSSA 区域。此选项仅在 NSSA 区域有效。

度量值类型： 配置发布的默认路由的度量值类型。支持两种类型：外部类型 1 和外部类型 2。默认为外部类型 2。外部类型 1 表示接收路由器在记录默认路由时将度量值设为下面的度量值加上自身到达本路由器的度量值，而外部类型 2 表示接收路由器在记录默认路由时将度量值设为下面的度量值。

度量值： 设置默认路由的度量值。合法范围是从 1 到 16777214，默认值为 1。

- **区域表**

在本页面中可以查看路由器当前连接的区域。

10.9.6 区域聚合

在本页面中，可以根据当前区域划分配置区域的聚合地址，用于在区域边界汇总路由信息。对于每一条活动的聚合地址，区域边界路由器（ABR）仅向其它区域发布一条聚合路由。

进入页面的方法： **路由功能>>OSPF>>区域聚合**

图 10-50 区域聚合

条目介绍:

- **配置区域聚合**

进程 ID: 选择配置区域的所属进程。

区域 ID： 唯一标识区域的 32 位无符号整数，可以是十进制格式或点分十进制格式。

IP 地址/子网掩码： 将指定区域的所有路由聚合成一个区域汇总地址。

开销： 配置区域聚合路由发布到其他区域时宣告的路由开销，如果没有设置，将由 OSPF 动态计算。

通告： 配置是否通过网络汇总 LSA 发布区域聚合路由到其它区域。

- **区域聚合地址表**

在本页面中可以查看交换机当前配置的区域聚合地址。

10.9.7 虚连接

如果交换机为一台非骨干区域的 ABR，且其连接的区域没有与骨干区域直接相连，则需要在交换机上配置虚连接与骨干区域 ABR 建立邻接关系。

进入页面的方法： **路由功能>>OSPF>>虚连接**

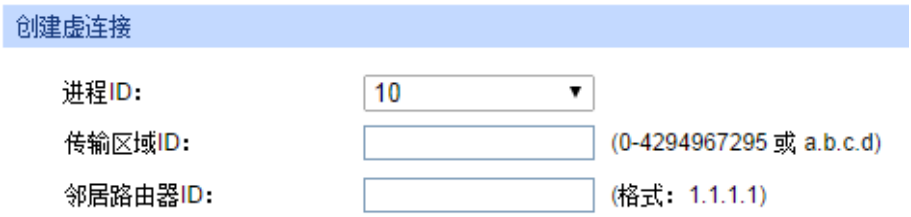


图 10-51 虚连接

条目介绍:

- **创建虚连接**

进程 ID:	选择配置区域的所属进程。
传输区域 ID：	配置虚连接需要穿透的区域。
邻居路由器 ID：	配置虚连接对端的邻居路由器的 ID。

- **虚连接表**

在本节中可以查看和管理已存在的虚连接。

进程:	选择查看指定进程的虚连接。
选择：	选择需要配置的条目，支持多选。
接口：	显示虚连接接口。当创建一条虚连接时，实际上创建了一个虚接口。
传输区域 ID：	显示虚连接的传输区域 ID。
邻居路由器 ID：	显示虚连接的邻居路由器 ID。
重传间隔：	配置虚接口的重传间隔，用于邻居之间重传 LSA 和 DD 报文。合法范围是从 1 到 65535，单位为秒，默认值为 5。
Hello 间隔：	接口发送 hello 报文的时间间隔，合法范围是从 1 到 65535，单位为秒，默认值为 10。此参数必须邻居路由器的邻接接口配置参数保持一致。
邻居失效间隔：	在指定时间内没有收到邻居的 hello 报文，路由器将宣告邻居失效的时间间隔，合法范围是从 1 到 65535，单位为秒，默认值为 40。
传输时延：	在虚连接接口上传输链路状态更新报文需要的时间，合法范围是从 1 到 65535，单位为秒，默认值为 1。

认证类型： 配置虚连接接口的认证类型，需要与邻居路由器上相应的接口认证类型一致，包含以下认证方式：

default：接口使用所属区域的认证方式。

null：不认证。

simple：简单密码认证。

md5：md5 加密认证。

简单密码： 输入用于简单认证的密码。

MD5 密码 ID： 输入用于 md5 加密认证的密码 ID。

MD5 密码 输入用于 md5 加密认证的密码。

状态： 显示虚连接接口的当前状态：

Down：此时接口没有与指定的邻居路由器形成邻接关系。

P2P：接口可用。接口要么与物理的点对点网络连接，要么是一条虚连接。路由器尝试与邻居路由器建立邻接关系，每隔 hello 间隔时间，就向邻居发送一个 hello 报文。

10.9.8 路由重发布

如果交换机上配置了多个 OSPF 进程或同时使能了多种路由协议，可以配置路由重发布特性，使不同进程或路由协议之间能够交换路由信息。

进入页面的方法： **路由功能>>OSPF>>路由重发布**

图 10-52 路由重发布

条目介绍:

- **路由重发布**

进程: 选择需要将路由信息发布到的目标 OSPF 进程。

选择： 勾选源进程或路由协议，不同 OSPF 进程或路由协议学习到的路由信息发布到目标 OSPF 进程时可以定义差异化的度量值、发布特征以及发布区域。

源： 显示源进程 ID 或路由协议。

重发布： 启用或禁用所选源进程或路由协议的路由重发布。

度量值： 配置重发布路由的度量值，有效值是从 1 到 16777214，默认值为在基本配置页面所设置的默认度量值。

度量值类型： 配置重发布路由的度量值类型。支持两种类型：外部类型 1 和外部类型 2。默认为外部类型 2。外部类型 1 表示交换机在记录重发布路由时将度量值设为上面的度量值加上自身到达邻接路由器的度量值，而外部类型 2 表示交换机在记录重发布路由时将度量值设为上面的度量值。

Tag： 设置重发布路由的 tag 域。合法范围是从 0 到 4294967295，默认值为 0。

仅 NSSA： 设置是否只发布路由到 NSSA 区域。默认禁用。

10.9.9 ASBR 聚合

在本页面中，可以配置 ASBR 的聚合地址，用于在自治系统边界汇总路由信息。对于每一条活动的聚合地址，自治系统边界路由器（ASBR）仅向 OSPF 域发布一条外部部由。

进入页面的方法： **路由功能>>OSPF>>ASBR 聚合**

图 10-53 ASBR 聚合

条目介绍:

- **配置 ASBR 聚合**

进程 ID: 选择需要配置聚合地址的 OSPF 进程。

IP 地址/子网掩码： 将指定进程的路由聚合成一个汇总地址。。

Tag： 设置发布聚合地址时的 tag 域。合法范围是 0 到 4294967295，默认值为 0。

仅 NSSA: 设置是否只发布聚合路由到 NSSA 区域。默认禁用。

通告： 设置是否启用通过一个 AS-External LSA 发布区域聚合路由到 OSPF 域。默认启用。

- **ASBR 聚合地址表**

在本节中可以查看和管理已存在的 ASBR 聚合地址。

10.9.10 邻居表

在本页面中，可以查看邻居列表。

进入页面的方法： **路由功能>>OSPF>>邻居表**

10.9.11 链路状态数据库

在本页面中，可以查看链路状态数据库。

进入页面的方法： **路由功能>>OSPF>>链路状态数据库**

10.9.12 配置步骤

运行了 OSPF 协议的路由设备根据其在网络中的不同位置，需要完成的工作各不相同， 而所需要完成的配置参数也各不相同。所有路由器均需要完成如下配置:

步骤	操作	说明
1	配置准备	在配置 OSPF 之前，需对网络做一个整体规划，确认 IR 所连接的网络以及相应的接口 IP 地址。
2	配置接口及 IP 地址	必选操作。在 **路由功能>>接口>>接口设置**页面中，根据路由器各接口连接的网络配置接口的网络层地址，使各相邻节点网络层可达。
3	创建 OSPF 进程	必选操作。在**路由功能>>OSPF>>进程配置**页面中，创建 OSPF 进程，并设置路由器 ID。
4	配置各路由接口所属的区域	必选操作。在**路由功能>>OSPF>>网络配置**页面中，指定网络接口所属的区域。IR 连接的网络需设置为同一区域。

针对 ABR 和 ASBR，在网络部署前期做好合理规划，还可以进行以下可选配置，降低网络中路由器上 LSDB 的大小，从而降低对路由器硬件的需求。

- **ABR 的可选配置**

步骤	操作	说明
1	配置虚链路	可选操作。当非骨干区域无法与骨干区域直接连接时，需要在非骨干区域 ABR 和骨干区域 ABR 之间配置虚链路。在**路由功能>>OSPF>>虚连接**页面中， 在非骨干区域 ABR 与骨干区域 ABR 上配置虚连接两端直连的区域参数以及对端路由器 ID。
2	配置区域内路由聚合	可选操作。当网络规模较大且前期规划较好时，在 ABR 上配置路由聚合能够减少通报到其他区域的路由条目，节约路由资源提高选路效率。在**路由功能>>OSPF>>区域聚合**页面中配置路由聚合。

- **ASBR 的可选配置**

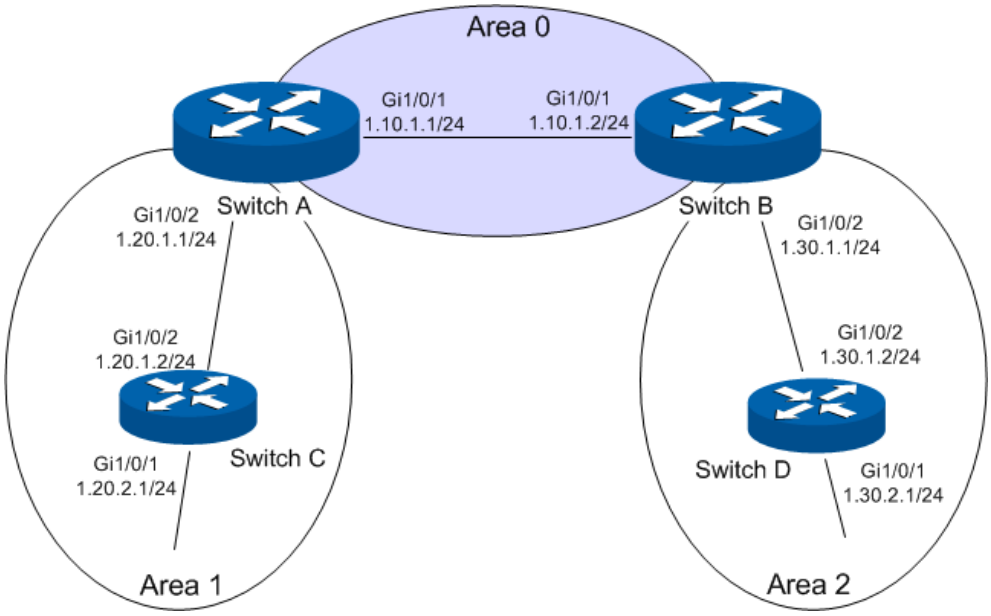
步骤	操作	说明
1	配置路由重发布	必选操作。如需要将其他路由协议的路由注入到 OSPF 路由，或将不同的 OSPF 进程间学习到的路由互相注入时，请配置路由重发布功能。在**路由功能>>OSPF>>路由重发布**页面中配置路由重发布。
2	配置 ASBR 路由聚合	可选操作。当网络规模较大且前期规划较好时，在 ASBR 上配置路由聚合能够减少通报到其他区域的路由条目，节约路由资源提高选路效率。在**路由功能>>OSPF>>ASBR 聚合**页面中配置 ASBR 路由聚合。

10.9.13 OSPF 功能组网应用

➢ **组网需求**

- 网络中所有的交换机都运行 OSPF，并将整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 配置完成后，每台交换机都应学到 AS 内的到所有网段的路由。

➢ **组网图**



➢ **配置步骤**

- 配置 Switch A

步骤	操作	说明
1	配置接口及 IP 地址	必选操作。在**路由功能>>接口>>接口设置**页面中，创建两个路由端口 1/0/1 和 1/0/2，并分别配置 IP 地址为 1.10.1.1/24、1.20.1.1/24。
2	创建 OSPF 进程	必选操作。在**路由功能>>OSPF>>进程配置**页面中，创建 OSPF 进程 1，并设置路由器 ID 为 1.1.1.1.
3	配置区域包含的网络	必选操作。在**路由功能>>OSPF>>网络配置**页面中，在区域 0 中配置网络 1.10.1.0 /24，在区域 1 中配置网络 1.20.1.0/24。
4	配置区域聚合	可选操作。在**路由功能>>OSPF>>区域聚合**页面中，在区域 1 中配置聚合地址 1.20.0.0 /16。

- 配置 Switch B

步骤	操作	说明
1	配置接口及 IP 地址	必选操作。在**路由功能>>接口>>接口设置**页面中，创建两个路由端口 1/0/1 和 1/0/2，并分别配置 IP 地址为 1.10.1.1/24、1.30.1.1/24。
2	创建 OSPF 进程	必选操作。在**路由功能>>OSPF>>进程配置**页面中，创建 OSPF 进程 1，并设置路由器 ID 为 2.2.2.2.
3	配置区域包含的网络	必选操作。在**路由功能>>OSPF>>网络配置**页面中，在区域 0 中配置网络 1.10.1.0 /24，在区域 2 中配置网络 1.30.1.0/24。

步骤	操作	说明
4	配置区域聚合	可选操作。在**路由功能>>OSPF>>区域聚合**页面中，在区域 2 中配置聚合地址 1.30.0.0 /16。

- 配置 Switch C

步骤	操作	说明
1	配置接口及 IP 地址	必选操作。在**路由功能>>接口>>接口设置**页面中，创建两个路由端口 1/0/1 和 1/0/2，并分别配置 IP 地址为 1.20.2.1/24、1.20.1.2/24。
2	创建 OSPF 进程	必选操作。在**路由功能>>OSPF>>进程配置**页面中，创建 OSPF 进程 1，并设置路由器 ID 为 3.3.3.3.
3	配置区域包含的网络	必选操作。在**路由功能>>OSPF>>网络配置**页面中，在区域 1 中配置网络 1.20.0.0 /16。

- 配置 Switch D

步骤	操作	说明
1	配置接口及 IP 地址	必选操作。在**路由功能>>接口>>接口设置**页面中，创建两个路由端口 1/0/1 和 1/0/2，并分别配置 IP 地址为 1.30.2.1/24、1.30.1.2/24。
2	创建 OSPF 进程	必选操作。在**路由功能>>OSPF>>进程配置**页面中，创建 OSPF 进程 2，并设置路由器 ID 为 4.4.4.4.
3	配置区域包含的网络	必选操作。在**路由功能>>OSPF>>网络配置**页面中，在区域 2 中配置网络 1.30.0.0 /16。

10.10 VRRP

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议。通常，一个网络内的所有主机都设置一条缺省路由，这样，主机发出的目的地址不在本网段的报文将通过缺省路由发往路由器 A，从而实现了主机与外部网络的通信。当路由器 A 发生故障时，本网段内所有以 A 为缺省路由下一跳的主机将断掉与外部的通信。

VRRP 就是为解决上述问题而提出的，它为具有多播或广播能力的局域网（如：以太网）设计。VRRP 将局域网的一组路由器（包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称之为一个备份组。

这个虚拟的路由器（即备份组）拥有自己的 IP 地址（这个 IP 地址可以和备份组内的某个路由器的接口地址相同，相同的则称为 IP 拥有者），备份组内的路由器也有自己的 IP 地址。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址，而并不知道具体的 Master 路由器的 IP 地址以及 Backup 路由器的 IP 地址，它们将自己的缺省路由设置为该虚拟路由器的 IP 地址。于是，网络内的主机就通过这个虚拟的路由器来与其它网络进行通信。当备份组内的 Master 路由器坏掉时，备份组内的其它 Backup 路由器将会通过选举策略选出一个新的 Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

- **VRRP 优点**

1. 简化网络管理。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息，也无需修改主机的默认网关配置。

2. 网络开销小。VRRP 只定义了一种报文——VRRP 通告报文，并且只有处于 Master 状态的路由器可以发送 VRRP 报文。

- **典型组网应用示例图**

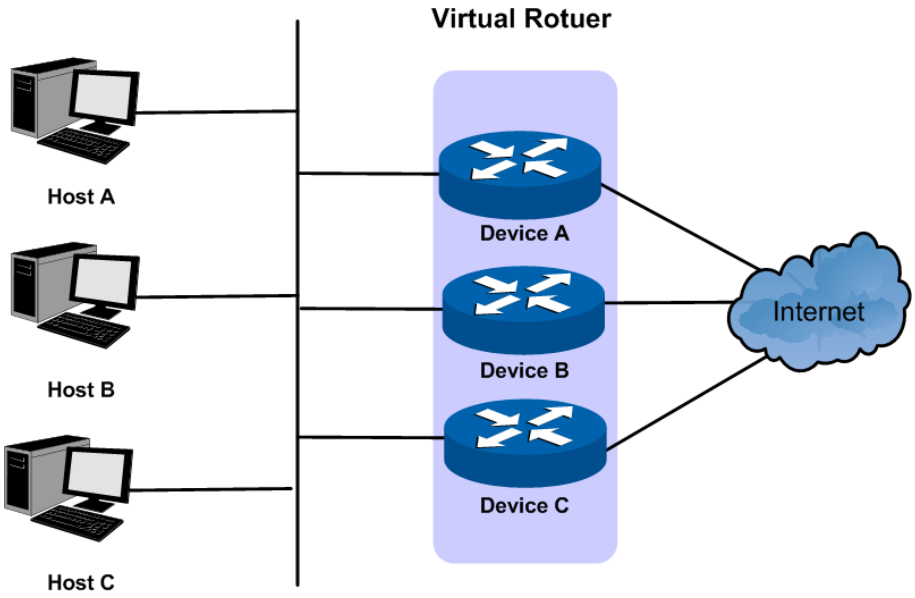


图 10-54 典型组网示意图

- **VRRP 工作原理**

1. 工作过程

VRRP 备份组，即虚拟路由器，由具有相同 VRID（虚拟路由器标识）的一组路由器构成。一个虚拟路由器拥有一个或多个虚拟 IP 地址，以及一个虚拟 MAC 地址（格式为 00-00-5E-00-01-{VRID}），局域网内的主机将虚拟路由器的 IP 地址设置为默认网关，通过虚拟路由器与外部网络进行通信。

虚拟路由器中的路由器根据优先级选举出 Master，Master 路由器将向网络内的主机提供路由服务，并周期性地发送 VRRP 报文，以向备份组中其他路由器公布其配置信息（优先级等）和工作状况。备份组中的其他路由器为 Backup 路由器，它们会监听 Master 发出的 VRRP 报文，并在 Master 出现故障时，选举出新的 Master，接替转发报文的工作。

2. Master 选举

初始创建的路由器工作在 Backup 状态，通过 VRRP 报文的交互获知虚拟路由器中其他成员的优先级。优先级最大的当选为 Master，若优先级相同，则比较接口的 IP 地址，IP 地址大的为 Master。

- 在抢占模式下，当 Backup 路由器收到 VRRP 通告报文后，会将自己的优先级与通告报文中的优先级进行比较。如果大于通告报文中的优先级，则成为 Master 路由器；否则将保持 Backup 状态。
- 在非抢占模式下，只要 Master 路由器没有出现故障，备份组中的路由器始终保持 Master 或 Backup 状态，Backup 路由器即使被配置成更高优先级也不会被选为 Master 路由器。

VRRP 优先级的取值范围为 0-255（数值越大表明优先级越高），可配置的范围是 1-254。优先级 0 为系统保留给路由器放弃 Master 位置时使用。例如，Master 接收到接口 Shutdown 的消息时，会向这个接口所在的 VRRP 组发送优先级为 0 的 VRRP 报文，主动放弃 Master 位置。255

则是系统保留给虚拟 IP 地址拥有者使用，当路由器为 IP 地址拥有者时，其优先级始终为 255。因此，当备份组内存在 IP 地址拥有者时，只要其工作正常，则为 Master 路由器。

3. 状态转换

VRRP 定义了三种状态模型：初始状态（Initialize）、活动状态（Master）和备份状态（Backup）。其中，只有 Master 状态可以为经过虚拟 IP 地址的转发请求提供服务以及发送 VRRP 报文。

系统刚启动时进入 Initialize 状态，如果没有给虚拟路由组配置虚拟 IP，则系统会一直保持 Initialize 状态。系统收到接口 startup 的消息后，如果虚拟 IP 地址配置正常，则转入 Backup（优先级不为 255 时）或 Master 状态（优先级为 255 时）。Master 或 Backup 状态的路由器只有在接收到接口 Shutdown 的消息时才会转为 Initialize 状态。在 Initialize 状态时，路由器不会处理 VRRP 报文。

Master 路由器在正常工作时，会定时发送 VRRP 报文，通知组内的备份路由器自己工作正常。用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 报文的时间间隔。如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 报文，则认为 Master 出现故障，将自己的状态改为 Master，并对外发送 VRRP 报文，重新进行 Master 选举。

为了避免备份组内的成员频繁进行主备份状态切换，让 Backup 路由器有足够的时间收集必要的信息（如路由信息），Backup 路由器接收到优先级低于本地优先级的 VRRP 报文后，不会立即抢占成为 Master，而是等待一定时间——抢占延迟时间后，才会对外发送 VRRP 报文取代原来的 Master 路由器。抢占延迟时间也可由用户自行设置。

4. 认证方式

VRRP 提供了三种认证方式：

- 无认证：不进行任何 VRRP 报文的合法性认证，不提供安全性保障。在一个安全的网络中，可以将认证方式设置为无认证。
- 简单字符认证：在一个有可能受到安全威胁的网络中，可以将认证方式设置为简单字符认证。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。
- MD5 认证：在一个非常不安全的网络中，可以将认证方式设置为 MD5 认证。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行摘要运算，运算结果保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字和 MD5 算法进行同样的运算，并将运算结果与认证头的内容进行比较。如果相同，则认为接收到的报文是合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

- **接口监视功能**

路由器连接上行链路的接口出现故障时，备份组无法感知上行链路的故障，如果该路由器此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。通过监视指定接口的功能，可以解决该问题。当连接上行链路的接口处于 Down 状态时，路由器主动降低自己的优先级，使得备份组内其它路由器的优先级高于这个路由器，以便优先级最高的路由器成为 Master，承担转发任务。

- **负载分担**

在路由器的一个接口上可以创建多个备份组，使得该路由器可以在一个备份组中作为 Master 路由器，在其他的备份组中作为 Backup 路由器。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的备份组，每个备份组都包括一个 Master 路由器和若干个 Backup 路由器，各备份组的 Master 路由器可以各不相同，如下图所示。

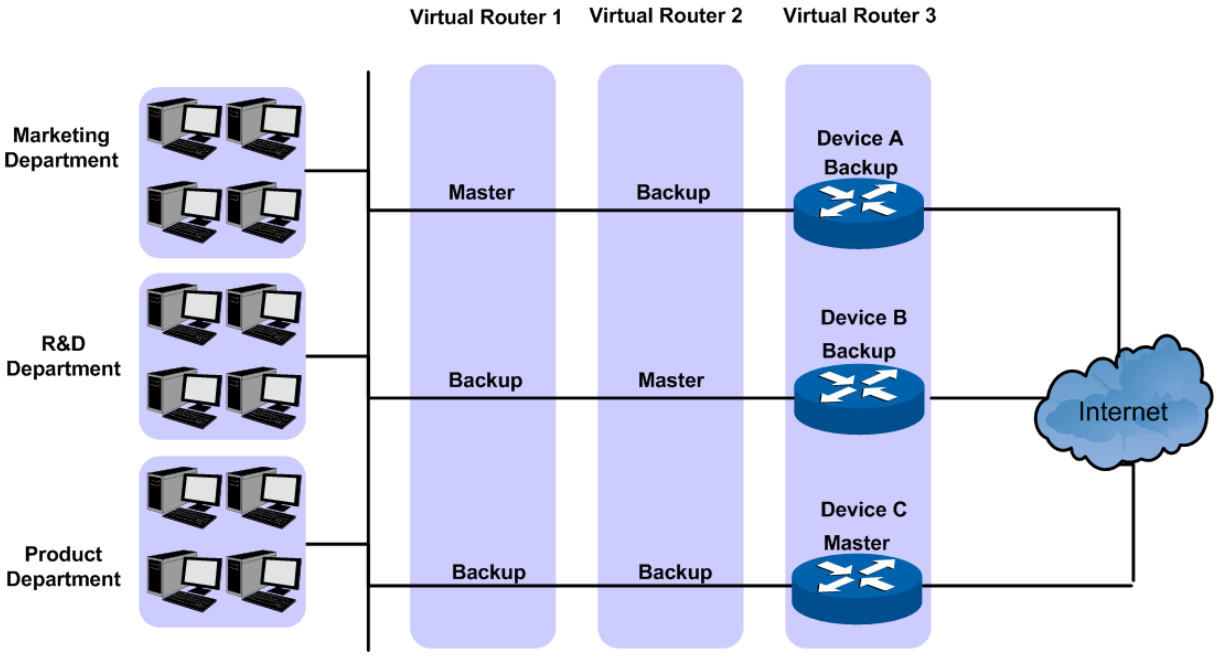


图 10-55 负载分担 VRRP

同一台路由器同时加入多个 VRRP 备份组，在不同备份组中有不同的优先级。

在上图中，有三个备份组存在：

- 备份组 1：对应虚拟路由器 1。Device A 作为 Master 路由器，Device B 和 Device C 作为 Backup 路由器。
- 备份组 2：对应虚拟路由器 2。Device B 作为 Master 路由器，Device A 和 Device C 作为 Backup 路由器。
- 备份组 3：对应虚拟路由器 3。Device C 作为 Master 路由器，Device A 和 Device B 作为 Backup 路由器。

为了实现业务流量在 Device A、Device B 和 Device C 之间进行负载分担，需要将局域网内的主机的默认网关分别设置为虚拟路由器 1、2 和 3。在配置优先级时，需要确保三个虚拟路由器中各路由器的 VRRP 优先级形成一定的交叉，使得一台路由器尽可能不同时充当 2 个 Master 路由器。

➢ **VRRP 配置**

用户配置 VRRP 前，需要做好前期规划工作，明确备份组内各成员设备的角色和功能。在备份组内的每个交换机上都需进行配置，才能形成一个备份组。

本功能包括**基本配置**、**高级配置**、**虚拟 IP 配置**、**接口监控配置**和**信息统计**五个配置页面。

10.10.1 基本配置

VRRP 是交换机的一项功能，它能动态指定局域网内的一台路由器成为虚拟路由器。Master 路由器控制虚拟路由的 IP 地址并承担报文转发任务。VRRP 功能使局域网内任意的 IP 地址都有可能成为终端主机的默认第一跳路由。

本页面用于配置 VRRP 和查看 VRRP 的状态信息。

进入页面的方法：**路由功能>>VRRP>>VRRP 基本配置**

图 10-56 VRRP 基本配置

条目介绍：

- **VRRP 基本配置**

VRID:	为新创建的 VRRP 设置一个 VRID 号，但在同一个接口下该 VRID 只能有一个。VRID 范围为:1-255。
接口:	为新创建的 VRRP 设置一个 VLAN 号。接口 ID 范围为:1-4094。
虚拟 IP:	为新创建的 VRRP 设置一个虚拟 IP。该虚拟 IP 格式为:0.0.0.0。
添加：	点击按钮添加新的 VRRP。
清空：	点击按钮清空当前 VRRP 设置。

- **VRRP 列表**

选择:	选择一个或者多个条目。
VRID:	显示相应 VRRP 的 VRID。
接口:	显示相应 VRRP 的接口 ID。
接口 IP:	显示相应 VRRP 的接口 IP 地址。
虚拟 IP:	显示相应 VRRP 的虚拟主 IP，如果没有设置虚拟 IP 地址，那么显示“—”。
优先级:	显示相应 VRRP 的优先级，默认优先级为 100。
状态:	显示相应 VRRP 所处的状态。
其他:	显示相应 VRRP 更多的信息。
全选：	选择所有条目。
删除：	删除所选择的条目。
刷新：	更新 VRRP 条目的状态。

点击<详细>按键，您可以看到所选虚拟路由的详细信息。

图 10-57 查看所选虚拟路由的详细信息

条目介绍：

- **所选 VRRP 的详细信息**

VRID：	显示相应 VRRP 的 VRID。
接口：	显示相应 VRRP 的接口 ID。
描述：	为相应 VRRP 设置描述信息。描述信息支持字母、数字和下划线，且最大可输入 8 个字符。
网络接口：	显示相应 VRRP 的接口 IP 地址。
状态：	显示相应 VRRP 所处的状态。
配置优先级：	显示相应 VRRP 的配置优先级。优先级的范围为：1-255。
运行优先级：	显示相应 VRRP 当前运行优先级。优先级的范围为：1-255。
通告报文定时器：	显示相应 VRRP 的通告报文时间。通告报文时间范围为：1-255。
抢占延时定时器：	显示相应 VRRP 的抢占时延。当主路由器出现故障时，备份路由器抢占成为主路由器前的等待时间为抢占时延。抢占时延范围为:0-255。
抢占模式：	显示相应 VRRP 的抢占模式。
认证类型：	显示相应 VRRP 的认证类型。
密钥：	如果您选择了简单认证和 MD5 认证，那么显示相应的认证密钥，否则，显示“—”。
虚拟 IP：	显示相应 VRRP 配置的所有虚拟 IP。
虚拟 MAC：	显示相应 VRRP 配置的虚拟 MAC。该虚拟 MAC 与 VRID 相对应。

10.10.2 高级配置

本页面用于配置虚拟路由的高级参数，包括描述、优先级、抢占模式、通告报文时间等。但不能添加或删除虚拟路由。

进入页面的方法：**路由功能>>VRRP>>高级配置**

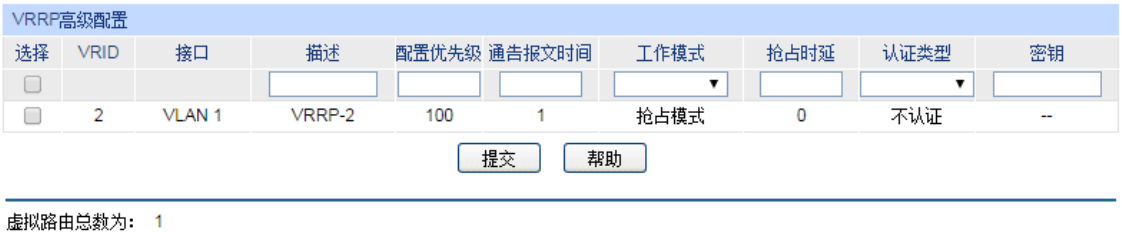


图 10-58 VRRP 高级配置

条目介绍：

- **VRRP 详细配置**

选择: 选择一个或者多个条目。

VRID: 显示相应 VRRP 的 VRID。

接口: 显示相应 VRRP 的接口 ID。

描述: 为相应 VRRP 设置描述信息。描述信息支持字母、数字和下划线，且最大可输入 8 个字符。

配置优先级: 配置相应 VRRP 的优先级。优先级的范围为：1-255。

通告报文时间: 配置相应 VRRP 的通告报文时间。通告报文时间范围为：1-255。

抢占模式: 可以从下拉列表中选择抢占模式和非抢占模式，当 backup 优先级高于 master 的优先级，处于抢占模式的 backup 会转为 master 状态。默认为抢占模式。

抢占时延: 设置相应 VRRP 的抢占时延。抢占时延范围为:1-255。

认证类型: 从下拉列表中选择相应的认证类型。默认为不认证。

- 不认证：不进行任何认证。
- 简单认证：需要设置相应的认证密钥。
- MD5：需要设置相应的认证密钥。

密钥: 如果您选择了简单认证和 MD5 认证，那么需要输入相应的认证密钥。

提交: 点击提交修改。

10.10.3 虚拟 IP 配置

本页面用于配置虚拟路由 IP。虚拟 IP 必须在虚拟路由的接口的子网内，您可以增加、删除或修改虚拟 IP。

进入页面的方法：**路由功能>>VRRP>>虚拟 IP 配置**

图 10-59 虚拟 IP 配置

条目介绍：

- **添加虚拟 IP**

  接口： 从下拉列表中选择一个接口 ID。

  VRID： 从下拉列表中选择一个 VRID。

  虚拟 IP： 键入相应的虚拟 IP，最多可以添加 5 个。

  添加： 点击此按钮为相应的 VRRP 增加虚拟 IP。

- **VRRP 虚拟 IP 列表**

  选择： 选择一个或者多个条目。

  VRID： 显示相应 VRRP 的 VRID。

  接口： 显示相应 VRRP 的接口 ID。

  虚拟 IP： 显示相应 VRRP 的虚拟 IP。

  提交： 修改相应 VRRP 的虚拟 IP。一次最多可以修改 1 个虚拟 IP。

  删除： 删除选中的虚拟 IP。

10.10.4 接口监控配置

本页面用于配置虚拟路由的监控接口。接口状态对于作为虚拟路由的交换机来说是重要的，接口 Up 状态出现的频率越高，交换机成为 Master 的可能性越大。

进入页面的方法：**路由功能>>VRRP>>接口监控配置**

图 10-60 接口监控配置

条目介绍：

- **添加监控接口**

接口： 从下拉列表中选择一个接口 ID。

VRID: 从下拉列表中选择一个 VRID。

监控接口： 输入要监控接口的 ID。

下降优先级： 监控接口为“down”时，需要降低的 VRRP 优先级。

添加： 点击此按钮添加监控接口。

- **接口监控列表**

选择： 选择一个或者多个条目。

VRID: 显示相应 VRRP 的 VRID。

接口： 显示相应 VRRP 的接口 ID。

监控接口： 配置和显示相应 VRRP 的监控接口 ID。

下降优先级： 配置和显示相应 VRRP 的监控接口的下降优先级。

接口状态： 显示监控接口的状态。

提交： 修改相应 VRRP 的监控接口。每次提交只能选择 1 个条目。

删除： 删除选中的接口。

刷新： 更新监控接口的连接状态。

10.10.5 信息统计

此页面用于显示 VRRP 的全局统计信息，包括 VRRP 校验和错误数、VRRP 版本信息错误数和 VRRP VRID 错误数等。

进入页面的方法：**路由功能>>VRRP>>信息统计**

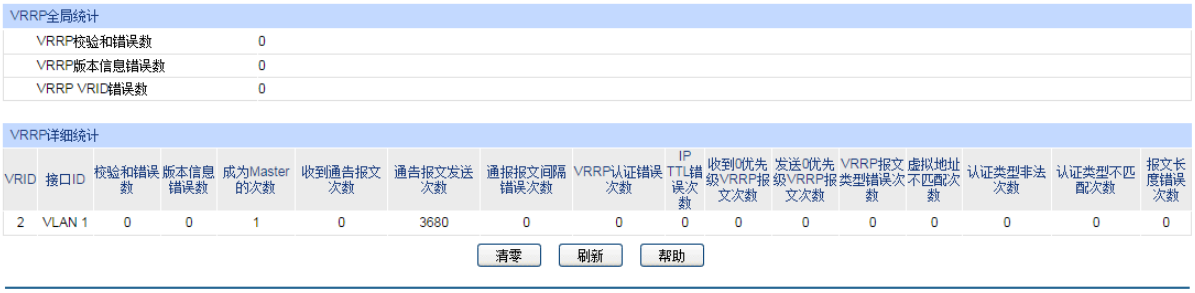


图 10-61 信息统计

条目介绍：

- **VRRP 全局统计**

  VRRP 校验和错误数： 统计所有 VRRP 收到的由于校验和错误导致的非法 VRRP 数据包。

  VRRP 版本信息错误数： 统计所有 VRRP 收到的由于版本错误导致的非法 VRRP 数据包。

  VRRP VRID 错误数： 统计所有VRRP收到的由于VRID不匹配导致的非法VRRP数据包。

- **VRRP 详细统计**

  VRID： 显示进行统计的 VRID

  接口 ID： 显示进行统计的接口 ID。

  校验和错误数： 显示该 VRRP 收到的由于校验和错误导致的非法 VRRP 数据包。

  版本信息错误数： 显示该 VRRP 收到的由于版本错误导致的非法 VRRP 数据包。

  成为 Master 的次数： 显示该 VRRP 状态称为 master 的次数。

  收到通告报文次数： 显示该 VRRP 收到通告报文的次数。

  通告报文发送次数： 显示该 VRRP 发送通告报文的次数。

  通告报文间隔错误次数： 显示该 VRRP 收到的 VRRP 包的通告报文时间间隔与本 VRRP 通告报文时间间隔不同的次数。

  VRRP 认证错误次数： 显示该 VRRP 收到的 VRRP 包认证失败的次数。

  IP TTL 错误次数： 显示该 VRRP 收到的 VRRP 包的 TTL 并不等于 255 的次数。

  收到 0 优先级 VRRP 报文次数： 显示该 VRRP 收到 VRRP 包是 0 优先级的次数。

  发送 0 优先级 VRRP 报文次数： 显示该 VRRP 发送 0 优先级 VRRP 报文的次数。

  虚拟地址不匹配次数： 显示收到的 VRRP 包的虚拟 IP 地址与本地虚拟 IP 地址不匹配的次数。

  认证类型非法次数： 显示收到的 VRRP 包的认证类型非法的次数。

  认证类型不匹配次数： 显示收到的 VRRP 包的认证类型与本地认证类型不匹配的次数。

报文长度错误次数： 显示收到的报文的长度小于 VRRP 头的次数。

清零： 清除上一次的统计结果。

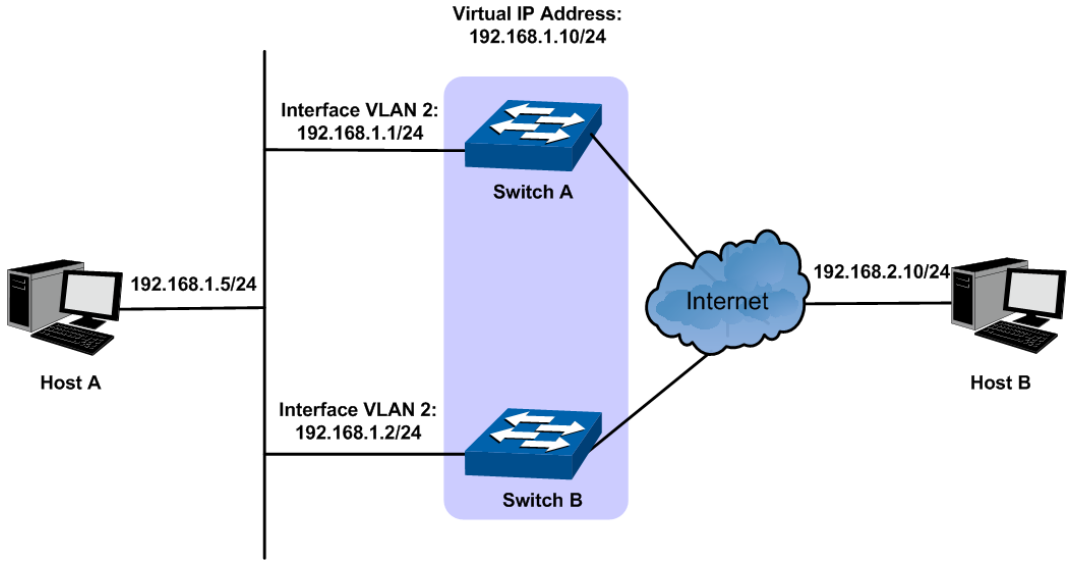
刷新： 刷新网页获取最新的统计结果。

10.10.6 VRRP 功能组网应用

➢ **组网需求**

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 192.168.1.10/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 192.168.1.10/24 的备份组；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

➢ **组网图**



➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	配置接口及 IP 地址	在**路由功能>>接口>>接口设置**页面，创建接口 VLAN2，并配置接口 IP 地址为：192.168.1.1/24。
2	端口加入接口	在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面，创建 VLAN 2，成员端口为 1/0/5。
3	创建 VRRP	在**路由功能>>VRRP>>基本配置**页面，创建 VRRP 实例，其中：VRID 配置为 1，接口配置为 VLAN2，虚拟 IP 配置为 192.168.1.10。
4	配置 VRRP 优先级	在**路由功能>>VRRP>>高级配置**页面，配置 VRRP 优先级为 110。

- 配置交换机 B：

步骤	操作	说明
1	配置接口及 IP 地址	在**路由功能>>接口>>接口设置**页面，创建 VLAN2，并配置接口 IP 地址为 192.168.1.2/24。
2	端口加入接口	在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面，创建 VLAN 2，成员端口为 1/0/5 号。
3	创建 VRRP	在**路由功能>>VRRP>>基本配置**页面，创建 VRRP 实例，其中：VRID 配置为 1，接口配置为 VLAN2，虚拟 IP 为 192.168.1.10。

回目录

第11章 组播路由

➢ 组播路由协议概述

说明：

本章中所提到的路由器和路由器图标，代表了一般意义下的路由器或者运行了三层组播路由协议的交换机。

组播路由协议运行在三层组播设备之间，用于建立和维护组播路由，并正确、高效地转发组播数据包。组播路由建立了从一个数据源端到多个接收端的数据传输路径，即组播分发树。

组播路由表由一组（S，G）条目构成，其中（S，G）表示由组播源 S 到组播组 G 的路由信息。如果不指定组播源，此条目将被表示为（*，G），* 表示任意组播源。如果路由器支持多种组播路由协议，它的组播路由表中将包含多种组播路由协议生成的组播路由。

组播路由协议包括 IGMP，PIM，MSDP 和 DVMRP 等组播路由协议以及静态组播路由。

下文中提到的域即指自治系统（Autonomous System）：一组使用相同路由协议交换路由信息的路由器，缩写为 AS。

IGMP 是 Internet Group Management Protocol（互联网组管理协议）的简称。它是 TCP/IP 协议族中负责 IP 组播成员管理的协议，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

PIM（Protocol Independent Multicast，协议无关组播）是目前较为典型的域内组播路由协议，利用静态路由或者任意单播路由协议（包括 RIP（路由信息协议）、OSPF（开放式最短路径优先协议）、IS-IS（中间系统到中间系统的路由选择协议）、BGP（边界网关协议）等）所生成的单播路由表为 IP 组播提供路由。

MSDP 是 Multicast Source Discovery Protocol（组播源发现协议）的简称，是为了解决多个 PIM SM（Protocol Independent Multicast Sparse Mode，协议无关组播—稀疏模式）域之间的互连而开发的一种域间组播解决方案，用来发现其它 PIM SM 域内的组播源信息。

DVMRP 是 Distance Vector Multicast Routing Protocol（距离矢量组播路由协议）的简称，主要应用于因特网组播主干网络。

下文主要介绍 IGMP，PIM 和静态组播路由。

➢ 组播角色和组播模型

在组播信息的传输方式中，各部分角色如下：

- 组播源（Multicast Source）：组播信息的发送者。
- 组播组成员（Multicast Group Member）：组播信息的所有接收者。
- 组播组（Multicast Group）：所有组播组成员构成一个组播组。
- 组播路由器（或称三层组播设备）：支持三层组播功能的路由器或者交换机。它们提供组播路由功能和对组播组成员的管理功能。

根据是否有明确的组播源，组播模型可以分为两类：ASM（任意信源组播）和 SSM（指定信源组播）。

ASM (Any-Source Multicast): 任意信源组播。在 ASM 中任意一个发送者都可以作为组播源向某个组播组地址发送信息，接收者可以加入由这个组播组地址标识的组播组，并接收发往这个组播组的

组播信息。ASM 模型中接收者无法事先知道组播源的位置，但可以在任何时间加入或离开该组播组。在任一特定的时刻，任意信源组播中的组播源不应该多于一个，否则可能造成网络拥塞和组播用户的误操作。

SSM(Source-Specific Multicast)：指定信源组播。SSM 模型中的接收者已经提前知道了组播源的具体位置。SSM 模型使用与 ASM 模型不同的组播组地址范围，它需要同时使用组播组地址和组播源地址来标识一个组播会话，并直接在接受者与其指定的组播源之间建立专用的组播转发路径。

11.1 全局配置

全局配置用于配置组播路由的全局参数和查看组播路由表。本功能包括**全局配置**和**组播路由表**两个配置页面。

11.1.1 全局配置

使能 IP 组播路由功能之后，交换机可以转发组播数据包，并建立自己的组播路由表。

进入页面的方法：**组播路由>>全局配置>>全局配置**

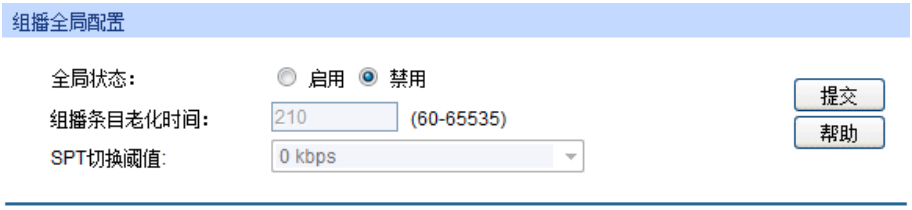


图 11-1 组播全局配置

条目介绍：

- **组播全局配置**

全局状态：	配置全局组播路由功能，缺省情况下，IP 组播路由功能处于关闭状态。
组播条目老化时间：	配置组播条目的老化时间。取值范围是 60 到 65535 秒。
SPT 切换阈值：	配置组播数据是利用 SPT 转发还是利用 RPT 转发。 若配置为“0 kbps”，组播数据便沿着 SPT 从发送者向接收者转发，而不“借道”RP； 若配置为“无限大”，则不会进行 SPT 切换。即：组播数据以 SPT 方式发送到 RP，再沿着 RPT 从 RP 发送到接收者。

11.1.2 组播路由表

此页面用表格展示组播路由总表，您可以通过设置搜索条件来进行搜索。

进入页面的方法：**组播路由>>全局配置>>组播路由表**

图 11-2 组播路由表

条目介绍：

- **搜索选项**

全部：	选择以显示所有组播路由条目。
组：	选择组并输入您要搜索的组播组地址。
源：	选择源并输入您要搜索的组播源地址。.
VLAN 接口：	入接口选择为 VLAN 接口并输入其 VLAN ID。
路由接口：	入接口选择为路由接口并输入或选择对应的端口。

- **组播路由表**

组：	组播组 IP 地址。
源：	组播源 IP 地址。 组播源和组播组 IP 地址可以确定一个唯一的组播条目。
入接口：	组播数据的入接口。
存活时间：	组播条目自创建以来的存活时间。
有效时间：	组播条目还可以存活的时间。此时间结束后该条目将会从组播表里移除。
RPF 邻居：	RPF 邻居的 IP 地址。
协议类型：	生成此条目的组播协议类型，包括 PIM DM 和 PIM SM。
条目类型：	当协议类型为 PIM SM 时此字段才有意义，条目类型包括 RPT 和 SPT。若为其他协议类型，则显示为“------”。
出接口：	组播路由转发的出口列表。

11.2 IGMP 配置

- **IGMP 简介**

IGMP 是 Internet Group Management Protocol（互联网组管理协议）的简称。它是 TCP/IP 协议族中负责 IPv4 网络中组播成员管理的协议，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

IGMP 目前有三个版本：

- IGMPv1（由 RFC 1112 定义）
- IGMPv2（由 RFC 2236 定义）
- IGMPv3（由 RFC 3376 定义）

所有版本的 IGMP 都支持 ASM 模型；IGMPv3 可以直接应用于 SSM 模型。

➢ **IGMPv1 工作机制**

IGMPv1 主要基于查询和响应机制来完成对组播组成员的管理。

当一个网段内有多台组播路由器时，由于它们都能从主机那里收到 IGMP 成员关系报告报文（Membership Report Message），因此只需要其中一台路由器负责发送 IGMP 查询报文（Query Message），此时需要有一个查询器（Querier）的选举机制来确定由哪台路由器作为 IGMP 查询器。

在 IGMPv1 中，由组播路由协议（如 PIM）选举出唯一的组播信息转发者 DR（Designated Router，指定路由器）作为 IGMP 查询器。

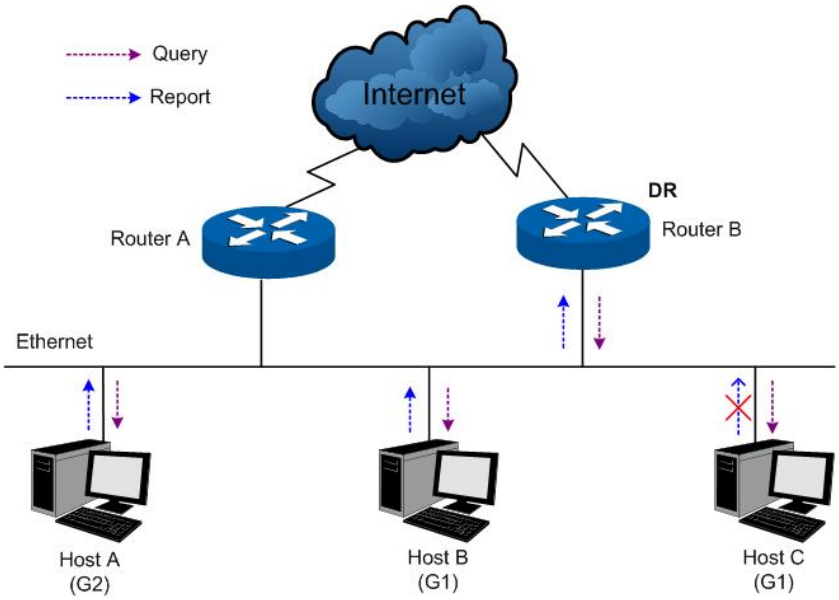


图 11-3 IGMP 查询与响应

如图 11-3 所示，假设 Host B 与 Host C 想要收到发往组播组 G1 的组播数据，而 Host A 想要收到发往组播组 G2 的组播数据，那么主机加入组播组以及 IGMP 查询器（Router B）维护组播组成员关系的基本过程如下：

(1) 主机会主动向其要加入的组播组发送 IGMP 成员关系报告报文以声明加入，而不必等待 IGMP 查询器发来的 IGMP 查询报文；

(2) IGMP 查询器周期性地以组播方式向本地网段内的所有主机与路由器发送 IGMP 查询报文（目的地址为 224.0.0.1）；

(3) 在收到该查询报文后，关注 G1 的 Host B 与 Host C 其中之一（这取决于谁的延迟定时器先超时）——比如 Host B，会首先以组播方式向 G1 发送 IGMP 成员关系报告报文，以宣告其属于 G1。由于本地网段中的所有主机和路由器都能收到 Host B 发往 G1 的报告报文，因此当 Host C 收到该报告报文后，将不再发送同样针对 G1 的报告报文，因为 IGMP 路由器（Router A 和

Router B）已知道本地网段中有对 G1 感兴趣的主机了。这个机制称为主机上的 IGMP 成员关系报告抑制机制，该机制有助于减少本地网段的信息流量；

(4) 与此同时，由于 Host A 关注的是 G2，所以它仍将以组播方式向 G2 发送报告报文，以宣告其属于 G2；

(5) 经过以上的查询和响应过程，IGMP 路由器了解到本地网段中有 G1 和 G2 的成员，于是由组播路由协议（如 PIM）生成（*，G1）和（*，G2）组播转发项作为组播数据的转发依据，其中的“*”代表任意组播源；

(6) 当由组播源发往 G1 或 G2 的组播数据经过组播路由到达 IGMP 路由器时，由于 IGMP 路由器上存在（*，G1）和（*，G2）组播转发项，于是将该组播数据转发到本地网段，接收者主机便能收到该组播数据了。

IGMPv1 没有专门定义离开组播组的报文。当运行 IGMPv1 的主机离开某组播组时，将不会向其要离开的组播组发送报告报文。当网段中不再存在该组播组的成员后，IGMP 路由器将收不到任何发往该组播组的报告报文，于是 IGMP 路由器在一段时间之后便会删除该组播组所对应的组播转发项。

- **IGMPv2 工作机制**

与 IGMPv1 相比，IGMPv2 增加了查询器选举机制和离开组机制。

1. 查询器选举机制

在 IGMPv2 中，查询器选举的过程如下：

(1) 所有 IGMPv2 路由器在初始时都认为自己是查询器，并向本地网段内的所有主机和路由器发送 IGMP 普遍组查询（General Query）报文（目的地址为 224.0.0.1）；

(2) 本地网段中的其它 IGMPv2 路由器在收到该报文后，将报文的源 IP 地址与自己的接口地址作比较。通过比较，IP 地址最小的路由器将成为查询器， 其它路由器成为非查询器（Non-Querier）；

(3) 所有非查询器上都会启动一个定时器（即其它查询器存在时间定时器 Other Querier Present Timer）。在该定时器超时前，如果收到了来自查询器的 IGMP 查询报文，则重置该定时器；否则，就认为原查询器失效，并发起新的查询器选举过程。

2. 离开组机制

在 IGMPv2 中，当一个主机离开某组播组时：

(1) 该主机向本地网段内的所有组播路由器（目的地址为 224.0.0.2）发送离开组（Leave Group）报文；

(2) 当查询器收到该报文后，向该主机所声明要离开的那个组播组发送特定组查询（Group-Specific Query）报文（目的地址字段和组地址字段均填充为所要查询的组播组地址）；

(3) 如果该网段内还有该组播组的其它成员，则这些成员在收到特定组查询报文后，会在该报文中所设定的最大响应时间（Max Response Time）内发送成员关系报告报文；

(4) 如果查询器在最大响应时间内收到了该组播组其它成员发送的成员关系报告报文，就会继续维护该组播组的成员关系；否则，查询器将认为该网段内已无该组播组的成员，于是不再维护这个组播组的成员关系。

➢ IGMPv3 工作机制

IGMPv3 在兼容和继承 IGMPv1 和 IGMPv2 的基础上，进一步增强了主机的控制能力，并增强了查询和报告报文的功能。

1. 主机控制能力的增强

IGMPv3 在特定组查询的基础上增加了针对组播源的过滤模式（INCLUDE/EXCLUDE），使主机在加入某组播组 G 的同时，能够明确要求接收或拒绝来自某特定组播源 S 的组播信息。当主机加入组播组时：

- 若要求只接收来自指定组播源如 S1、S2、……的组播信息，则其报告报文中可以标记为 INCLUDE Sources（S1，S2，……）；
- 若拒绝接收来自指定组播源如 S1、S2、……的组播信息，则其报告报文中可以标记为 EXCLUDE Sources（S1，S2，……）。

如图 11-4 所示，网络中存在 Source 1（S1）和 Source 2（S2）两个组播源，均向组播组 G 发送组播报文。Host B 仅对从 Source 1 发往 G 的信息感兴趣，而对来自 Source 2 的信息没有兴趣。

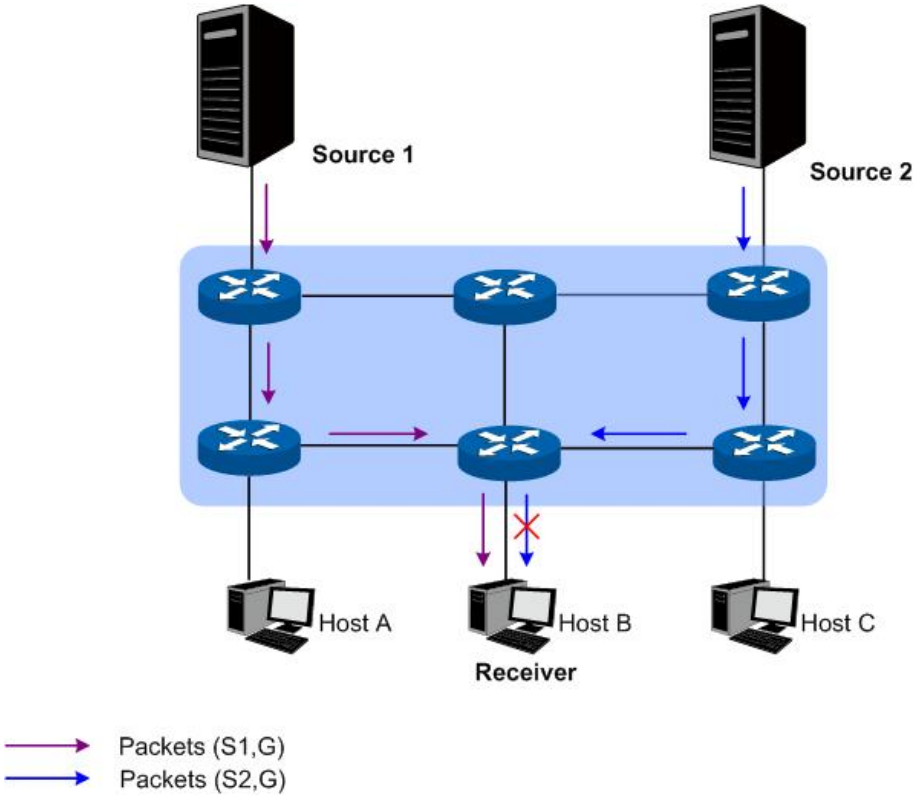


图 11-4 IGMPv3 组播源过滤

如果主机与路由器之间运行的是 IGMPv1 或 IGMPv2，Host B 加入组播组 G 时无法对组播源进行选择，因此无论 Host B 是否需要，来自 Source 1 和 Source 2 的组播信息都将传递给 Host B。

当主机与路由器之间运行了 IGMPv3 之后，Host B 就可以要求只接收来自 Source 1 发往 G 的组播信息（S1，G），或要求拒绝来自 Source 2 发往 G 的组播信息（S2，G），这样就只有来自 Source 1 的组播信息才能传递给 Host B 了。

2. 查询和报告报文功能的增强

(1) 携带源地址的查询报文

IGMPv3 不仅支持 IGMPv1 的普遍组查询和 IGMPv2 的特定组查询，而且还增加了对特定源组查询的支持：

- 普遍组查询报文中，既不携带组地址，也不携带源地址；
- 特定组查询报文中，携带组地址，但不携带源地址；
- 特定源组查询报文中，既携带组地址，还携带一个或多个源地址。

(2) 包含多组记录的报告报文

IGMPv3 报告报文的目的地址为 224.0.0.22，可以携带一个或多个组记录。在每个组记录中，包含有组播组地址和组播源地址列表。组记录可以分为多种类型，如下：

- IS_IN：表示组播组与组播源列表之间的对应方式为 INCLUDE，即只接收从指定组播源列表发往该组播组的组播数据。如果此时的指定组播源列表为空，则表示离开该组播组。
- IS_EX：表示组播组与组播源列表之间的对应方式为 EXCLUDE，即只接收从指定组播源列表之外的组播源发往该组播组的组播数据。
- TO_IN：表示组播组与组播源列表之间的对应方式由 EXCLUDE 转变为 INCLUDE。
- TO_EX：表示组播组与组播源列表之间的对应方式由 INCLUDE 转变为 EXCLUDE。
- ALLOW：表示在现有状态的基础上，还希望从某些组播源接收组播数据。如果当前的对应关系为 INCLUDE，则向现有组播源列表中添加这些组播源；如果当前的对应关系为 EXCLUDE，则从现有组播源列表中删除这些组播源。
- BLOCK：表示在现有状态的基础上，不再希望从某些组播源接收组播数据。如果当前的对应关系为 INCLUDE，则从现有组播源列表中删除这些组播源；如果当前的对应关系为 EXCLUDE，则向现有组播源列表中添加这些组播源。

IGMP 配置用于配置 IGMP 接口和报文的相关参数，以及静态组播组和组播组过滤器等功能。本功能包括**接口配置**，**接口状态**，**静态组播组配置**，**组播组显示**，**Profile 绑定**和**报文统计**等六个配置页面。

11.2.1 接口配置

此页面用来配置 IGMP 接口，您可以通过设置搜索条件来进行筛选。

进入页面的方法：**组播路由>>IGMP 配置>>接口配置**

图 11-5 接口配置

条目介绍：

- **搜索选项**

全部：	选择以显示所有的 IGMP 接口条目。
VLAN 接口：	输入需要显示的 VLAN 接口 ID 值。
环回接口：	输入需要显示的环回接口 ID 值。.
路由接口：	输入需要显示的路由接口 ID 值。

- **IGMP 接口配置**

选择：	选择需要配置的虚拟接口。
接口：	虚拟接口的名称，虚拟接口在配置 IGMP 前应配置 IP 地址。
管理模式：	IGMP 使能状态。您可以启用或禁用所选中虚拟接口的 IGMP 功能。
版本号：	配置此接口上运行的 IGMP 版本。 • IGMPv1：虚拟接口运行 IGMPV1 版本。 • IGMPv2：虚拟接口运行 IGMPV2 版本。 • IGMPv3：虚拟接口运行 IGMPV3 版本。
鲁棒值：	配置所选中的 IGMP 接口的鲁棒值。
查询间隔：	配置普通组查询间隔。
最大响应时间：	配置查询报文所携带的最大响应时间。
初始查询间隔：	当 IGMP 刚启用时，发送查询报文的间隔。
初始查询个数：	当 IGMP 刚启用时，按照初始查询间隔所发送的查询报文数量。
最后成员查询间隔：	当组播组最后一个成员离开时，IGMP 发送特殊组查询报文间隔。
最后成员查询次数：	当组播组最后一个成员离开时，IGMP 发送特殊组查询报文数量。
查询器有效时间：	配置查询器有效时间。如果非查询器在此时间超时前没有收到来自查询器的 IGMP 查询报文，就会认为原有的查询器失效，从而触发新的查询器选举过程。
检查路由警告：	启用此功能，IGMP 将丢弃未携带路由警告的报文。
发送路由警告：	启用此功能，IGMP 将发送携带路由警告的报文。

11.2.2 接口状态

您可以在此页面上设置搜索条件，只显示特定类型的接口。

进入页面的方法：**组播路由>>IGMP 配置>>接口状态**

图 11-6 接口状态

条目介绍：

- **搜索选项**

  全部： 选择以显示所有的 IGMP 接口条目。

  VLAN 接口： 输入需要显示的 VLAN 接口 ID 值。

  环回接口： 输入需要显示的环回接口 ID 值。.

  路由接口： 输入需要显示的路由接口 ID 值。

- **接口状态**

  接口： 虚拟接口的名称，虚拟接口在配置 IGMP 前应配置 IP 地址。

  IP 地址： 接口的 IP 地址。

  查询器 IP： 该接口的查询器的 IP 地址。

  查询器状态： 该接口的查询器所处于的状态。

  其他查询器老化时间： 其他查询器的老化时间，以秒为单位。如果本地接口是查询器，则该值为 0。

  组播组数目： 该接口当前加入的动态组播组数目。

11.2.3 静态组播组配置

您可以在此页面配置静态组播组条目。静态组播组条目不会通过 IGMP 协议学习到，不受动态条目和组播过滤功能的影响。组播地址从 224.0.0.1 到 239.255.255.255。接收者可以加入的组播组地址由 224.0.1.0 到 239.255.255.255。

进入页面的方法：**组播路由>>IGMP 配置>>静态组播组配置**

图 11-7 IGMP 静态组播组

条目介绍：

- **IGMP 静态组播组**

  接口： 输入需要配置的接口 ID，VLAN 接口 ID 或路由端口。

  组播组 IP： 输入组播组 IP 地址。

  源 IP： 输入组播源 IP 地址。

- **搜索选项**

  搜索选项： 选择需要显示组播组列表的规则，以便快速寻找需要设置的组播组条目。

  - 全部：选择以显示所有的静态组播组条目。
  - 组播组 IP：输入组播组 IP 来显示该组播 IP 下的静态组播组条目。
  - VLAN 接口：输入 VLAN 接口 ID 来显示该 VLAN 接口下的静态组播组条目。
  - 转发端口：输入转发端口来显示包含该转发端口的静态组播组条目。
  - 路由端口：输入路由端口来显示该路由端口下的静态组播组条目。

- **静态组播组列表**

  接口： 显示接口信息。

组播组 IP： 显示静态组播组的组播地址。

源 IP： 显示组播条目的源 IP 地址。.

转发端口： 显示组播条目的转发端口。

11.2.4 组播组显示

在 IP 组播环境下，所有的接收者都能加入到某个组播组中。您可以在这个页面查看本机的组播组信息。组播地址范围是 224.0.0.1 到 239.255.255.255。接收者可以加入的组播组地址为 224.0.1.0 到 239.255.255.255。

进入页面的方法：**组播路由>>IGMP 配置>>组播组显示**

图 11-8 组播组显示

条目介绍：

- **搜索选项**

搜索选项： 选择需要显示组播组列表的规则，以便快速寻找需要设置的组播组条目。

- 全部：选择以显示所有的组播组条目。
- 组播组 IP：输入组播组 IP 来显示该组播 IP 下的组播组条目。
- VLAN 接口：输入 VLAN 接口 ID 来显示该 VLAN 接口下的组播组条目。
- 转发端口：输入转发端口来显示包含该转发端口的组播组条目。
- 路由端口：输入路由端口来显示该路由端口下的组播组条目。

- **组播组显示**

接口： 显示接口信息。

组播组 IP： 显示组播组的组播地址。

转发端口： 显示组播条目的转发端口。

操作： 点击显示按钮显示组播条目的模式和源 IP 地址。

11.2.5 Profile 绑定

当端口接收 IGMP 报告报文时，交换机根据报文检查端口上配置的组播过滤地址 ID，如果组播地址未被过滤，则将这个端口加入到该组播组的转发端口列表中，否则交换机就丢弃该 IGMP 报告报文，从而控制了用户所能加入的组播组。此页面上的 Profile 绑定配置和**组播过滤**功能共享。

进入页面的方法：**组播路由>>IGMP 配置>>Profile 绑定**

图 11-9 Profile 与最大加入组播数目绑定

条目介绍：

- **Profile 与最大加入组数目绑定**

UNIT：	选择堆叠中需要配置的成员。
端口：	选择需要配置的端口。
Profile ID：	与端口绑定的 Profile ID 列表。
最大加入组数目：	端口允许加入的最大组播组数目。
溢出操作：	当端口所加入组播组数等于或超过最大组播组数时采取的动作。 • 丢弃：端口不再加入新的组播组。 • 替换：端口加入新的组播组，并将端口从当前已加入的组播组 IP 地址最小的组播组中移除。
LAG：	显示端口当前所属的汇聚组。
清除绑定：	清除端口绑定的 Profile。
Profile：	点击此按钮来创建新的 IGMP Profile。

图 11-10 创建 IGMP Profile

条目介绍：

- **创建 IGMP Profile**

  Profile ID： 输入您想创建的 Profile ID，取值范围为 1-999。

  模式： 配置 Profile 的过滤模式。
  - 允许：只允许加入 Profile 中 IP 地址范围内的组播组。
  - 拒绝：拒绝加入 Profile 中 IP 地址范围的组播组。

- **显示设置**

  全部： 显示所有的 IGMP Profile 条目。

  Profile ID： 显示包含所输入的 Profile ID 的条目。

- **IGMP Profile 信息**

  Profile ID： 显示 Profile ID。

  模式： 显示 Profile 的过滤模式。
  - 允许：只允许加入 Profile 中 IP 地址范围内的组播组。
  - 拒绝：拒绝加入 Profile 中 IP 地址范围的组播组。

  绑定端口： 显示该 Profile 所绑定的端口列表。

  操作： 点击该按钮可以配置该 Profile 的模式和过滤 IP 地址区间。

图 11-11 Profile 配置

条目介绍：

- **Profile 模式**

  Profile ID： 显示您要配置的 Profile ID。

  模式： 配置 Profile 的过滤模式。
  - 允许：只允许加入 Profile 中 IP 地址范围内的组播组。
  - 拒绝：拒绝加入 Profile 中 IP 地址范围的组播组。

- **添加 IP 范围**

  起始地址： 输入 IP 地址区间的起始 IP 地址。

  结束地址： 输入 IP 地址区间的结束 IP 地址。

- **IP 范围**

  序号： 显示 IP 地址区间的序号。

  起始地址： 输入 IP 地址区间的起始 IP 地址。

  结束地址： 输入 IP 地址区间的结束 IP 地址。

11.2.6 报文统计

您可以在本页查看交换机各接口的组播报文流量信息，便于您监控网络中 IGMP 报文。

进入页面的方法：**组播路由>>IGMP 配置>>报文统计**

图 11-12 IGMP 报文统计

条目介绍：

- **自动刷新**

自动刷新：	选择是否启用自动刷新功能。
刷新周期：	填写自动刷新的时间周期。

- **报文统计**

接口：	显示接口。
查询报文：	显示接口接收到的查询报文的数目。
报告报文（V1）	显示接口接收到的 IGMPv1 报告报文的数目。
报告报文（V2）	显示接口接收到的 IGMPv2 报告报文的数目。
报告报文（V3）	显示接口接收到的 IGMPv3 报告报文的数目。
离开报文	显示接口接收到的离开报文的数目。
错误报文	显示接口接收到的错误报文的数目。
刷新：	点击此按钮来手动刷新报文统计列表。

IGMP 配置步骤：

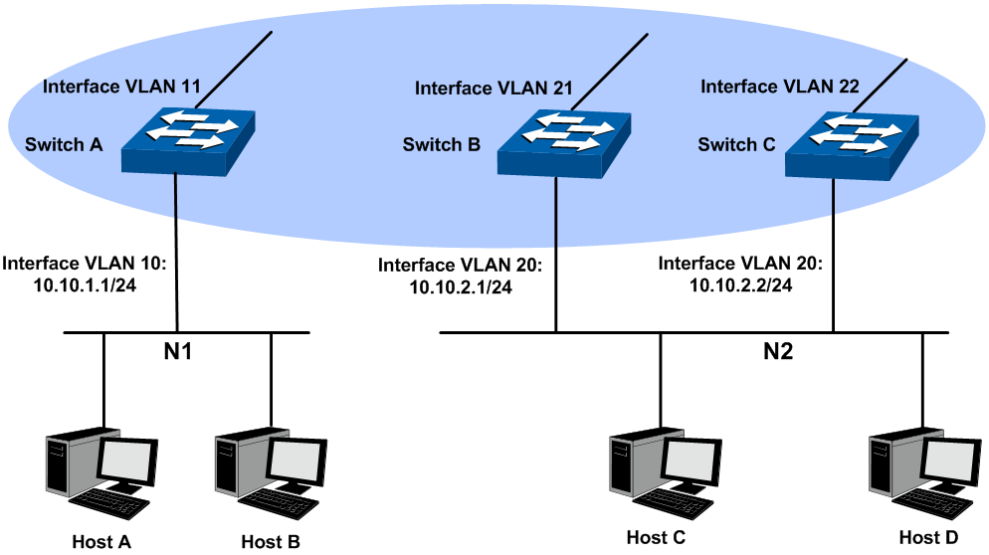
步骤	操作	说明
1	使能 IP 组播路由	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由。
2	使能 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能接口的 IGMP 功能并选择 IGMP 版本。

11.2.7 IGMP 功能的组网应用

- **组网需求**

- 不同组织的接收者组成末梢网络 N1 和 N2，Host A 和 Host C 分别是 N1 和 N2 中的组播信息接收者。他们通过组播方式接收视频点播信息。
- PIM 网络中交换机 A 连接 N1，交换机 B 与交换机 C 共同连接 N2。
- 交换机 A 通过 VLAN 接口 10 连接 N1，通过 VLAN 接口 11 连接 PIM 网络中的其他设备。
- 交换机 B 和交换机 C 分别通过各自的 VLAN 接口 20 连接 N2；交换机 B 通过 VLAN 接口 21 连接 PIM 网络中其他设备，交换机 C 通过 VLAN 接口 22 连接 PIM 网络中其他设备。
- 交换机 A 与 N1 之间运行 IGMPv3 协议；交换机 B 和交换机 C 与 N2 之间运行 IGMPv2 协议，并由交换机 B 充当 IGMP 查询器。

➢ **组网图**



➢ **配置步骤**

1) 配置接口的 IP 地址和单播路由协议。

按组网图来配置各个接口的 IP 地址和子网掩码。具体配置过程此处略去。

配置各交换机之间采用 OSPF 协议进行互连，确保 PIM 网络中交换机 A，交换机 B 和交换机 C 能够在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新。具体配置过程此处略去。

2) 使能 IP 组播路由，并在用户侧接口上使能 IGMP 功能。

- 配置交换机 A

步骤	操作	说明
1	使能 IP 组播路由	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由。
2	在用户侧接口上使能 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能 VLAN 接口 10 的 IGMPv3 功能。

- 配置交换机 B

步骤	操作	说明
1	使能 IP 组播路由	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由。
2	在用户侧接口上使能 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能 VLAN 接口 20 的 IGMPv2 功能。

- 配置交换机 C

步骤	操作	说明
1	使能 IP 组播路由	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由。
2	在用户侧接口上使能 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能 VLAN 接口 20 的 IGMPv2 功能。

11.3 PIM DM

本节先综述 PIM 协议的特点，RPF 检查机制和 PIM 的两种模式，然后详细介绍 PIM DM 的工作机制。

PIM 是目前较为常用的域内组播路由协议，它不依赖于某一特定的单播路由协议，而是利用静态路由或者任意单播路由协议（包括路由信息协议（RIP）、开放式最短路径优先协议（OSPF）、中间系统到中间系统协议（IS-IS）、边界网关协议（BGP）等）所生成的单播路由表为 IP 组播提供路由。

与其他路由协议不同，PIM 不需要在路由器之间更新路由信息，它并不会构造一个独立的路由转发表，只是借助 RPF（Reverse Path Forwarding，逆向路径转发）检查机制来实现对组播报文的转发。

在组播实现中，组播路由和转发分为两种表：

- 各组播路由协议的组播路由信息经过综合形成一个总的组播路由表（Multicast Routing-Table）；
- 组播转发表（Multicast Forwarding-Table）直接用于控制组播数据包的转发。

组播路由表由一组（S，G）表项组成，其中（S，G）表示由源 S 向组播组 G 发送组播数据的路由信息；若不限定组播源，则用（*，G）表示，“*”表示来自任意组播源。如果路由器支持多种组播路由协议，则其组播路由表中将包括由多种协议生成的组播路由。路由器根据组播路由和转发策略，从组播路由表中选出最优的组播路由，并下发到组播转发表中。

组播路由协议在创建组播路由表项时，运用了 RPF 机制，从而确保组播数据能够沿正确的路径传输。

➢ **RPF Mechanism**

PIM 协议主要利用单播路由表来进行 RPF 检查。RPF 机制除了可以保证正确地按照组播路由的配置转发组播报文外，还能避免由于各种原因而造成的环路。

1. RPF 检查

执行 RPF 检查的依据是单播路由或静态组播路由。单播路由表中汇集了到达各个目的网段的最短路径，而静态组播路由表中则列出了用户通过手工配置指定的静态 RPF 路由信息。组播路由协议并不独立维护某种单播路由，而是依赖于网络中现有的单播路由信息或静态组播路由来创建组播路由表项。

在执行 RPF 检查时，路由器同时查找单播路由表和静态组播路由表，具体过程如下：

(1) 首先分别从单播路由表和静态组播路由表中各选出一条最优路由：

- 以“报文源”的 IP 地址为目的地址查找单播路由表，自动选取一条最优单播路由。对应表项中的出接口为 RPF 接口，下一跳为 RPF 邻居。路由器认为来自 RPF 邻居且由该 RPF 接口收到的组播报文所经历的路径是从组播源 S 到本地的最短路径。
- 以“报文源”的 IP 地址为指定源地址查找静态组播路由表，自动选取一条最优静态组播路由。对应表项明确指定了 RPF 接口和 RPF 邻居。

(2) 然后从这两条最优路由中选择一条作为 RPF 路由：

根据默认的最长掩码匹配优先原则，将从这两条路由中选出最长掩码匹配的那条路由；如果这两条路由的掩码一样，则选择其中优先级最高的那条路由；如果它们的优先级也相同，则选择静态组播路由。

2. RPF 机制的应用

路由器在收到由组播源 S 向组播组 G 发送的组播报文后，首先查找组播转发表：

(1) 如果存在对应的（S，G）表项，且该报文实际到达的接口与组播转发表中的入接口一致，则向所有的出接口执行转发。

(2) 如果存在对应的（S，G）表项，但是该报文实际到达的接口与组播转发表中的入接口不一致，则对此报文执行 RPF 检查：

- 若检查结果表明 RPF 接口与现存（S，G）表项的入接口相同，则说明（S，G）表项正确，丢弃这个来自错误路径的报文；
- 若检查结果表明 RPF 接口与现存（S，G）表项的入接口不符，则说明（S，G）表项已过时，将入接口修改为该报文实际到达的接口，然后向所有的出接口转发。

(3) 如果不存在对应的（S，G）表项，则也对该报文执行 RPF 检查。将 RPF 接口作为入接口，结合相关路由信息创建相应的表项，并下发到组播转发表中：

- 如果该报文实际到达的接口正是 RPF 接口，则 RPF 检查通过，向所有的出接口执行转发；
- 如果该报文实际到达的接口不是 RPF 接口，则 RPF 检查失败，丢弃该报文。

➢ **PIM Modes**

根据路由机制的不同，PIM 分为以下两种模式：

- PIM DM（Protocol Independent Multicast-Dense Mode，协议无关组播—密集模式）
- PIM SM（Protocol Independent Multicast-Sparse Mode，协议无关组播—稀疏模式）

➢ **PIM DM**

PIM DM（在 RFC3973 中定义）属于密集模式的组播路由协议，使用“推（Push）模式”传送组播数据，通常适用于组播组成员相对比较密集的小型网络。

PIM DM 的基本原理如下：

- PIM DM 假设网络中的每个子网都存在至少一个组播组成员，因此组播数据将被扩散（Flooding）到网络中的所有节点。然后，PIM DM 对没有组播数据转发的分支进行剪枝（Prune），只保留包含接收者的分支。这种“扩散—剪枝”现象周期性地发生，被剪枝的分支也可以周期性地恢复成转发状态。
- 当被剪枝分支的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM DM 使用嫁接（Graft，见嫁接）机制主动恢复其对组播数据的转发。一般说来，密集模式下数据包的转发路径是有源树（Source Tree，即以组播源为“根”、组播组成员为“枝叶”的一棵转发树）。由于有源树使用的是从组播源到接收者的最短路径，因此也称为最短路径树（Shortest Path Tree，SPT）。

PIM DM 的工作流程可以概括如下：

- 邻居发现
- 构建 SPT
- 嫁接

➢ **邻居发现**

在 PIM 域中，路由器通过周期性地的向所有 PIM 路由器（224.0.0.13）以组播方式发送 PIM Hello 报文（以下简称 Hello 报文），以发现 PIM 邻居，维护各路由器之间的 PIM 邻居关系，从而构建和维护 SPT。

➢ **构建 SPT**

构建 SPT 的过程也就是“扩散—剪枝”的过程：

(1) 在 PIM DM 域中，组播源 S 向组播组 G 发送组播报文时，首先对组播报文进行扩散：路由器对该报文的 RPF 检查通过后，便创建一个（S，G）表项，并将该报文向网络中的所有下游节点转发。经过扩散，PIM DM 域内的每个路由器上都会创建（S，G）表项。

(2) 然后对那些下游没有接收者的节点进行剪枝：由没有接收者的下游节点向上游节点发剪枝报文（Prune Message），以通知上游节点将相应的接口从其组播转发表项（S，G）所对应的出接口列表中删除，并不再转发该组播组的报文至该节点。

说明：

（S，G）表项包括组播源的地址 S、组播组的地址 G、出接口列表和入接口等信息。

剪枝过程最先由叶子路由器发起，如图 11-13 所示，没有接收者（Receiver）的路由器（如与 Host C 直连的路由器）主动发起剪枝，并一直持续到 PIM DM 域中只剩下必要的分支，这些分支共同构成了 SPT。

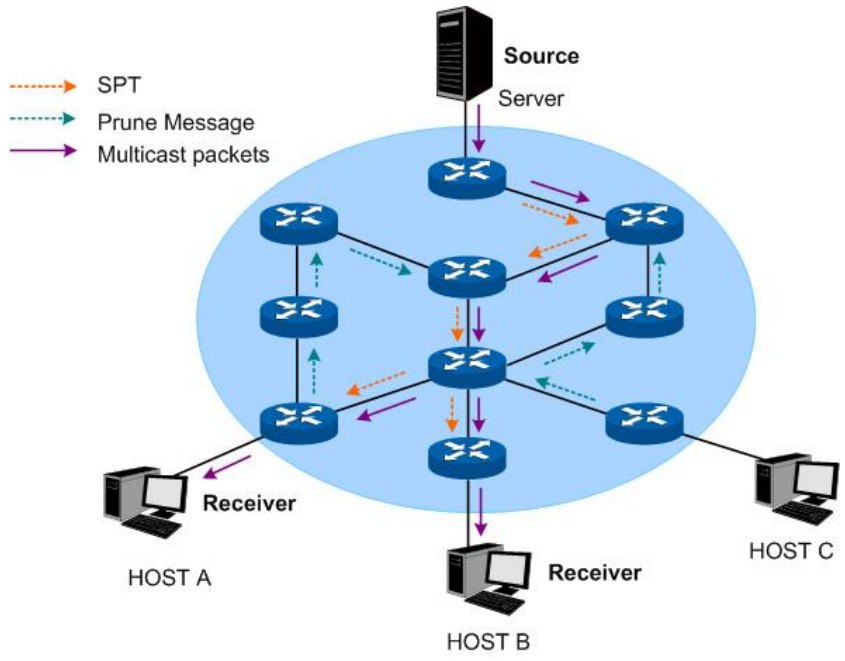


图 11-13 PIM DM 中的 SPT 拓扑

“扩散—剪枝”的过程是周期性发生的。各个被剪枝的节点提供超时机制，当剪枝超时后便重新开始这一过程。

➢ **嫁接**

当被剪枝的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM DM 使用嫁接机制主动恢复其对组播数据的转发，过程如下：

(1) 需要恢复接收组播数据的节点向组播源的方向逐跳发送嫁接报文（Graft Message）给其上游节点以申请重新加入到 SPT 中；

(2) 当上游节点收到该报文后恢复该下游节点的转发状态，并向其回应一个嫁接应答报文（Graft-Ack Message）以进行确认；

(3) 如果发送嫁接报文的下游节点没有收到来自其上游节点的嫁接应答报文，将重新发送嫁接报文直到被确认为止。

- **断言机制**

在一个网段内如果存在多台组播路由器，则相同的组播报文可能会被这些路由器重复发送到该网段。为了避免出现这种情况，就需要通过断言（Assert）机制来选定唯一的组播数据转发者。

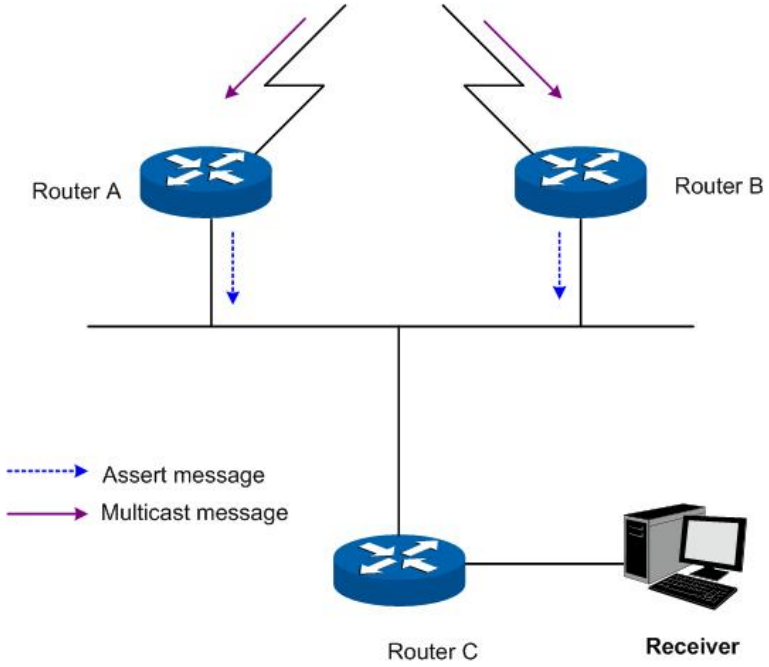


图 11-14 断言机制

如图 11-14 所示，当 Router A 和 Router B 从上游节点收到（S，G）组播报文后，都会向本地网段转发该报文，于是处于下游的节点 Router C 就会收到两份相同的组播报文，Router A 和 Router B 也会从各自的本地接口收到对方转发来的该组播报文。

此时，Router A 和 Router B 会通过本地接口向所有 PIM 路由器（224.0.0.13）以组播方式发送断言报文（Assert Message），该报文中携带有以下信息：组播源地址 S、组播组地址 G、到组播源的单播路由的优先级和度量值。通过一定的规则对这些参数进行比较后，Router A 和 Router B 中的获胜者将成为（S，G）组播报文在本网段的转发者，比较规则如下：

(1) 到组播源的单播路由的优先级较高者获胜；

(2) 如果到组播源的单播路由的优先级相等，那么到组播源的度量值较小者获胜；

(3) 如果到组播源的度量值也相等，则本地接口 IP 地址较大者获胜。

本功能包括 **PIM DM 接口配置**和 **PIM DM 邻居**两个配置页面。

11.3.1 PIM DM 接口配置

在此界面上可以使能接口的 PIM DM 功能并配置相关参数。

进入页面的方法：**组播路由>>PIM DM>>PIM DM 接口配置**

图 11-15 PIM DM 接口配置

条目介绍：

- **PIM DM 接口配置**

选择：	选择需要配置 PIM DM 功能的接口。
接口：	用来显示或者配置的接口。配置 PIM DM 之前需要到路由接口页面添加接口。
状态：	启用或禁用所选接口的 PIM DM 功能。
Hello 间隔：	指定 Hello 报文的发送间隔时间，单位为秒，默认值为 30 秒。
DR 优先级：	配置用于 DR 选举的 DR 优先级。
IP 地址：	显示接口的 IP 地址。
邻居数目：	显示接口的邻居数目。
DR 地址：	显示该接口上的 DR 的 IP 地址。

11.3.2 PIM DM 邻居

此页面显示 PIM 接口通过发送和接收 PIM Hello 报文所学习到的 PIM DM 邻居的信息。

进入页面的方法：**组播路由>>PIM DM>>PIM DM 邻居**

图 11-16 PIM DM 邻居

条目介绍：

- **搜索**

全部：	显示所有的 PIM 邻居。

接口： 显示指定接口上学习到的 PIM 邻居。

邻居： 显示包含指定邻居的条目。

➢ **PIM DM 邻居表**

接口： 显示接口。

邻居： 此接口上学习到的相关邻居的信息。

存活时间： 邻居生成时间，表示该邻居条目自创建以来的存活时间。。

老化时间： 邻居的老化时间，表示还有多长时间邻居会被老化掉。

刷新： 点击此按钮来刷新邻居列表。

PIM DM 配置步骤：

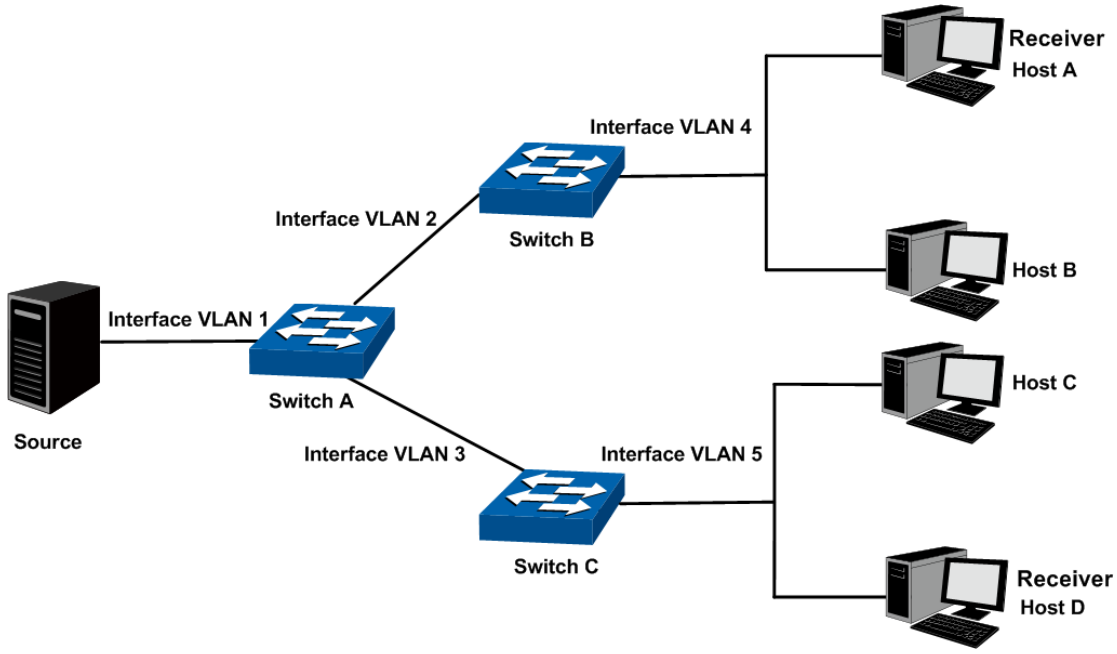
步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，配置路由接口的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。
3	使能组播路由和 PIM DM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM DM>>PIM DM 接口配置**界面上使能接口的 PIM DM 功能。
4	使能 IGMP	可选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能与组播接收者相连的路由接口的 IGMP 功能。

11.3.3 PIM DM 功能的组网应用

➢ **组网需求**

- 接收者通过组播来接收视频点播数据。整个网络中运行 PIM DM 作为组播路由协议。
- Host A 和 Host D 是组播接收者。
- 交换机 A 与交换机 B 通过 VLAN 接口 2 连接，交换机 A 与交换机 C 通过 VLAN 接口 3 连接。组播源服务器与交换机 A 通过 VLAN 接口 1 连接。
- Host A 与 Host B 通过 VLAN 接口 4 连接到交换机 B，Host C 与 Host D 通过 VLAN 接口 5 连接到交换机 C。
- 与 Host 相连的 VLAN 接口运行 IGMP 协议。

➢ **组网图**



各交换机中每个 VLAN 接口的 IP 地址如下所示：

交换机 A：VLAN 接口 1: 192.168.1.2/24

VLAN 接口 2: 192.168.2.2/24

VLAN 接口 3: 192.168.3.2/24

交换机 B：VLAN 接口 2: 192.168.2.100/24

VLAN 接口 4: 192.168.4.100/24

交换机 C：VLAN 接口 3: 192.168.3.100/24

VLAN 接口 5: 192.168.5.100/24

➢ **配置步骤**

- 配置交换机 A:

步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，配置 VLAN 接口 1，2 和 3 的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。
3	使能组播路由和 PIM DM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM DM>>PIM DM 接口配置**界面上使能 VLAN 接口 1，2 和 3 的 PIM DM 功能。

- 配置交换机 B 和 C：

步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，分别配置 VLAN 接口 2，3，4 和 5 的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。
3	使能组播路由和 PIM DM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM DM>>PIM DM 接口配置**界面上使能 VLAN 接口 2，3，4 和 5 的 PIM DM 功能。
4	使能 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能与组播接收者相连的 VLAN 接口 4 和 5 的 IGMP 功能。

11.4 PIM SM

PIM DM 使用以“扩散—剪枝”方式构建的 SPT 来传送组播数据。尽管 SPT 的路径最短，但是其建立的过程效率较低，并不适合大中型网络。

PIM SM 属于稀疏模式的组播路由协议，使用“拉（Pull）模式”传送组播数据，通常适用于组播组成员分布相对分散、范围较广的网络。

PIM SM 的基本原理如下：

- PIM SM 假设所有主机都不需要接收组播数据，只向明确提出需要组播数据的主机进行转发。PIM SM 实现组播转发的核心任务就是构造并维护 RPT（Rendezvous Point Tree，共享树或汇集树），RPT 选择 PIM 域中某台路由器作为公用的根节点 RP（Rendezvous Point，汇集点），组播数据通过 RP 沿着 RPT 转发给接收者；
- 连接接收者的路由器向某组播组对应的 RP 发送加入报文（Join Message），该报文被逐跳送达 RP，所经过的路径就形成了 RPT 的分支；
- 组播源如果要向某组播组发送组播数据，首先由与组播源直连的路由器负责向 RP 进行注册，把注册报文（Register Message）通过单播方式发送给 RP，该报文到达 RP 后触发建立 SPT。之后组播源把组播数据沿着 SPT 发向 RP，当组播数据到达 RP 后，被复制并沿着 RPT 发送给接收者。

说明：

复制仅发生在分发树的分支处，这个过程能够自动重复直到数据包最终到达接收者。

PIM SM 的工作流程可以概括如下：

- 邻居发现
- DR 选举
- RP 发现

- 构建 RPT
- 组播源注册
- RPT 向 SPT 切换
- 断言

➢ **邻居发现**

PIM SM 使用与 PIM DM 完全相同的邻居发现机制，具体请参见"邻居发现"一节。

➢ **DR 选举**

借助 Hello 报文可以为共享网络选举 DR（Designated Router，指定路由器），DR 将作为该共享网络中组播数据的唯一转发者。

无论是与组播源相连的网络，还是与接收者相连的网络，只要是共享网络，就需要选举 DR。接收者侧的 DR 负责向 RP 发送加入报文；组播源侧的 DR 负责向 RP 发送注册报文。

说明：

- 各路由器之间通过比较 Hello 报文中所携带的优先级和 IP 地址，可以为多路由器网段选举 DR。选举出的 DR 对于 PIM SM 有实际的意义；而对于 PIM DM 来说，其本身其实并不需要 DR，但如果 PIM DM 域中的共享网络上运行了 IGMPv1，则需要选举出 DR 来充当共享网络上的 IGMPv1 查询器。
- 在充当 DR 的设备上必须使能 IGMP，否则连接在该 DR 上的接收者将不能通过该 DR 加入组播组。

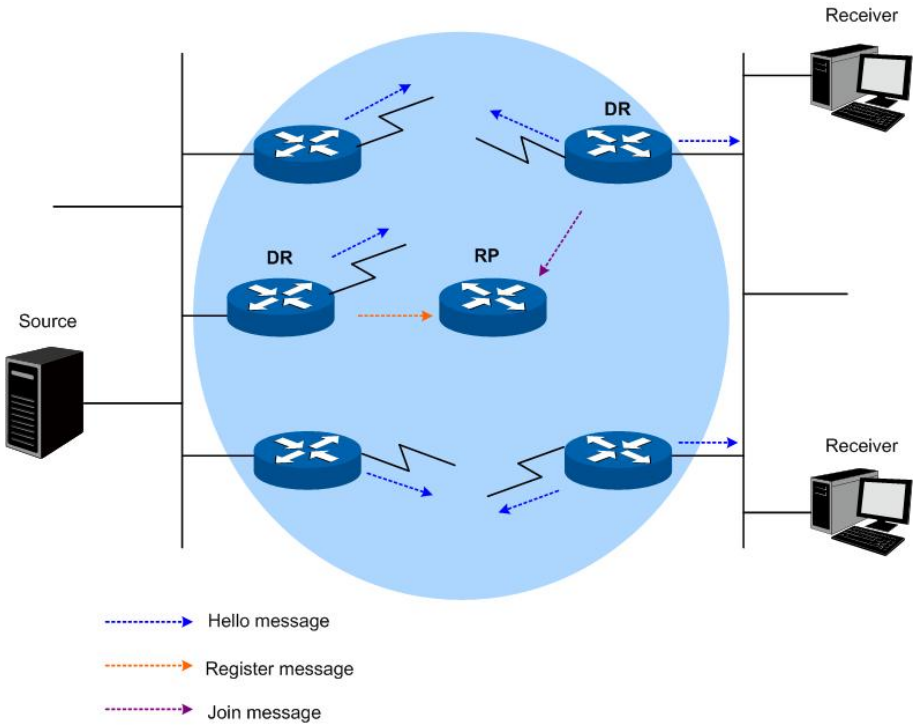


图 11-17 DR 选举

如图 11-17 所示，DR 的选举过程如下：

(1) 共享网络上的各路由器相互之间发送 Hello 报文（携带有竞选 DR 优先级的参数），拥有最高优先级的路由器将成为 DR；

(2) 如果优先级相同，或者网络中至少有一台路由器不支持在 Hello 报文中携带竞选 DR 优先级的参数，则根据各路由器的 IP 地址大小来竞选 DR，IP 地址最大的路由器将成为 DR。

当 DR 出现故障时，其余路由器在超时后仍没有收到来自 DR 的 Hello 报文，则会触发新的 DR 选举过程。

- **RP 发现**

RP 是 PIM SM 域中的核心设备。在结构简单的小型网络中，组播信息量少，整个网络仅依靠一个 RP 进行组播信息的转发即可，此时可以在 PIM SM 域中的各路由器上静态指定 RP 的位置；但是在更多的情况下，PIM SM 域的规模都很大，通过 RP 转发的组播信息量巨大。为了缓解 RP 的负担，并优化 RPT 的拓扑结构，不同的组播组应该对应不同的 RP，这就需要通过自举机制（bootstrapping mechanism）来动态选举 RP，此时需要配置 BSR（BootStrap Router，自举路由器）。

BSR 是 PIM SM 域中的管理核心，负责收集网络中由 C-RP（Candidate-RP，候选 RP）发来的宣告报文（Advertisement Message），然后为每个组播组选择部分 C-RP 信息以组成 RP-Set（RP 集，即组播组与 RP 的映射关系数据库），并发布到整个 PIM SM 域。网络中所有的路由器（包括 DR）能够根据这些 RP-Set 提供的信息算出所需 RP 的位置。

在一个 PIM SM 域（或管理域）内只能有一个 BSR（更多 BSR 管理域的介绍参考 BSR 管理域介绍），但可以配置多个 C-BSR（Candidate-BSR，候选 BSR）。这样，一旦 BSR 发生故障，其余 C-BSR 能够通过自动选举产生新的 BSR，从而确保业务免受中断。同样，一个 PIM SM 域内也可以配置多个 C-RP，并通过 BSR 机制计算出每个组播组所对应的 RP。RP 和 BSR 在网络中的位置如图 11-18 所示。

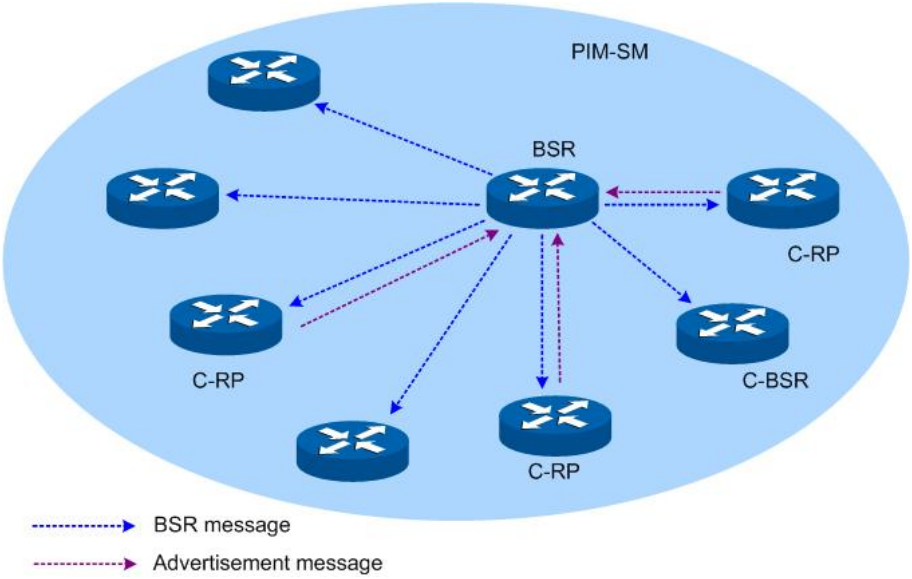


图 11-18 C-RP,C-BSR 和 BSR 在网络中的位置

- **构建 RPT**

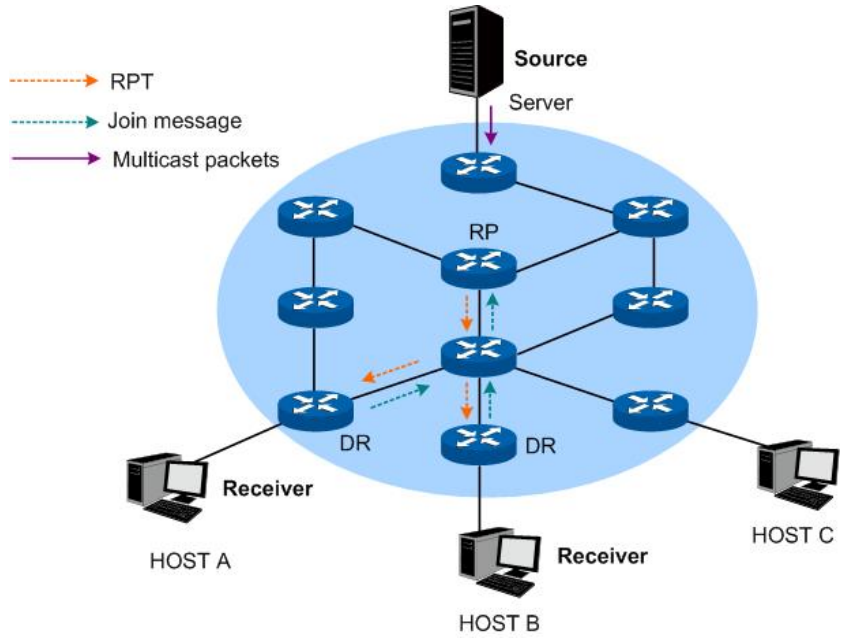


图 11-19 PIM SM 中的 RPT 拓扑

如图 11-19 所示，RPT 的构建过程如下：

(1) 当接收者加入一个组播组 G 时，先通过 IGMP 报文通知与其直连的 DR；

(2) DR 掌握了组播组 G 的接收者的信息后，向该组播组所对应的 RP 方向逐跳发送加入报文；

(3) 从 DR 到 RP 所经过的路由器就形成了 RPT 的分支，这些路由器都在其转发表中生成了（*，G）表项，这里的“*”表示来自任意组播源。RPT 以 RP 为根节点，以 DR 为叶子节点。

当发往组播组 G 的组播数据流经 RP 时，数据就会沿着已建立好的 RPT 到达 DR，进而到达接收者。

当某接收者对组播组 G 的信息不再感兴趣时，与其直连的 DR 会逆着 RPT 向该组的 RP 方向逐跳发送剪枝报文；上游节点收到该报文后在其接口列表中删除与下游节点之间的链路，并检查自己是否拥有该组播组的接收者，如果没有则继续向其上游转发该剪枝报文。

- **组播源注册**

组播源注册的目的是向 RP 通知组播源的存在。

如图 11-20 所示，组播源向 RP 注册的过程如下：

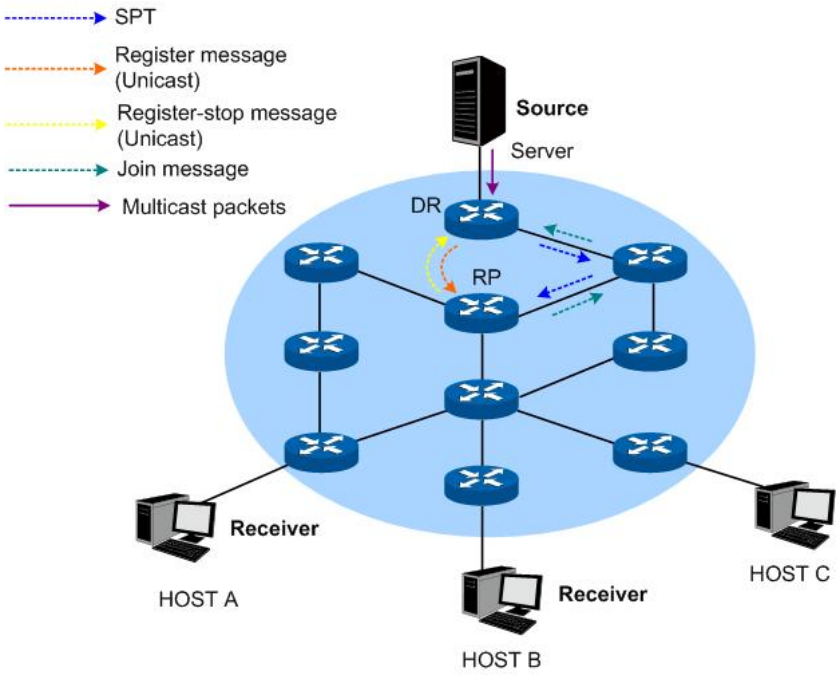


图 11-20 PIM SM 中的组播源注册拓扑图

(1) 当组播源 S 向组播组 G 发送了一个组播报文时，与组播源直连的 DR 在收到该报文后，就将其封装成注册报文，并通过单播方式发送给相应的 RP；

(2) 当 RP 收到该报文后，一方面解封装注册报文并将封装在其中的组播报文沿着 RPT 转发给接收者，另一方面向组播源逐跳发送（S，G）加入报文。这样，从 RP 到组播源所经过的路由器就形成了 SPT 的分支，这些路由器都在其转发表中生成了（S，G）表项。SPT 以组播源为根，以 RP 为叶子。

(3) 组播源发出的组播数据沿着已建立好的 SPT 到达 RP，然后由 RP 把组播数据沿着 RPT 向接收者进行转发。当 RP 收到沿着 SPT 转发来的组播数据后，通过单播方式向与组播源直连的 DR 发送注册停止报文（Register-Stop Message），组播源注册过程结束。

- **从 RPT 向 SPT 切换**

一旦接收者侧的 DR 接收到了 RP 发往组播组 G 的组播数据，就会发起从 RPT 向 SPT 的切换，过程如下：

(1) 接收者侧 DR 向组播源 S 逐跳发送（S，G）加入报文，并最终送达组播源侧 DR，沿途经过的所有路由器在其转发表中都生成了（S，G）表项，从而建立了 SPT 分支；

(2) 接收者侧 DR 向 RP 逐跳发送剪枝报文，RP 收到该报文后会将其向组播源方向转发，从而最终实现从 RPT 向 SPT 的切换。

从 RPT 切换到 SPT 后，组播数据将直接从组播源发送到接收者。通过由 RPT 向 SPT 的切换，PIM SM 能够以比 PIM DM 更经济的方式建立 SPT。

- **断言机制**

PIM SM 使用与 PIM DM 完全相同的断言机制，具体请参见“断言机制”一节。

➢ **BSR 管理域**

BSR 是 PIM SM 域中的管理核心，在一个 PIM SM 域内只能有一个 BSR，并由该 BSR 负责在整个 PIM SM 域内宣告 RP-Set 信息，所有组播组的信息都在此 BSR 管理的网络范围内进行转发。当 PIM SM 域较大时，可以考虑将整个 PIM SM 域划分为多个 BSR 管理域，一方面可以有效分担单一 BSR 的管理压力，另一方面可以为特定组播组提供专门的服务。

在地域空间上，各 BSR 管理域之间相互隔离，即同一路由器不能从属于多个 BSR 管理域。换句话说，各 BSR 管理域所包含的路由器互不相同。

在组播地址上，每个 BSR 管理域为特定的组播组提供服务，这些组播组地址之间通常没有交集，但是也可能存在相互交叉和重叠关系，如下图 11-21 所示。

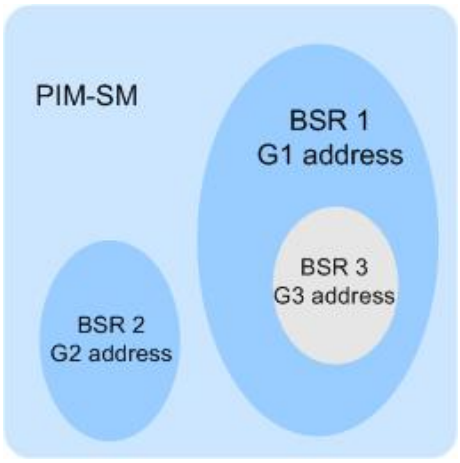


图 11-21 由组播组划分的 BSR 域

BSR 管理域的特点：

- 通过设置 BSR 边界来实现不同的管理域。每个 BSR 管理域都有自己的边界，都包含针对各自域的 C-RP 和 BSR 设备，这些设备仅在所在域有效，也就是说 BSR 机制与 RP 选举在各管理域之间是隔离的；
- BSR 消息穿透不了 BSR 域，各 BSR 管理域内的组播信息（如 C-RP 宣告报文、BSR 自举报文等）不能跨越域边界。

PIM SM 用于配置 PIM SM 接口和候选 BSR，BSR，候选 RP，静态 RP 等参数。本功能包括 **PIM SM 接口配置**，**PIM SM 邻居**，**BSR**，**RP**，**RP 映射**和 **RP 信息**六个配置页面。

11.4.1 PIM SM 接口配置

在此界面上可以使能接口的 PIM SM 功能并配置相关参数。

进入页面的方法：**组播路由>>PIM SM>>PIM SM 接口配置**

PIM SM接口配置

选择	接口	状态	Hello间隔	Join/Prune间隔	DR优先级	BSR边界	IP地址	邻居数目	DR地址
	Vlan1	禁用	30	60	1	禁用	192.168.0.5	---	---
	Gi1/0/23	禁用	30	60	1	禁用	1.20.1.1	---	---
	Gi1/0/24	禁用	30	60	1	禁用	1.10.1.1	---	---

提交 帮助

图 11-22 PIM SM 接口配置

条目介绍：

- **搜索**

全部：	选择需要配置 PIM SM 功能的接口。
接口：	显示可供配置的接口。
状态：	选择开启或关闭 PIM SM 功能。
Hello 间隔：	指定 Hello 报文的发送间隔时间，单位为秒，默认值为 30 秒。
Join/Prune 间隔：	指定接口的 Join/Prune 报文发送时间间隔。配置范围是 1 到 18724 秒，默认值是 60 秒。
DR 优先级：	指定 DR 的优先级。默认值为 1。
BSR 边界：	选择开启或关闭 PIM 的边界功能。
IP 地址：	显示该接口的 IP 地址。
邻居数目：	显示该接口的邻居数目。
DR 地址：	显示该接口的 DR 的地址。

11.4.2 PIM SM 邻居

此页面显示 PIM 接口通过发送和接收 PIM Hello 报文所学习到的 PIM SM 邻居的信息。

进入页面的方法：**组播路由>>PIM SM>>PIM SM 邻居**

图 11-23 PIM SM 邻居

条目介绍：

- **搜索**

全部：	显示所有的 PIM 邻居。
VLAN 接口：	显示指定 VLAN 接口上学习到的 PIM 邻居。
路由端口：	显示指定路由端口上学习到的 PIM 邻居。
邻居：	显示包含指定邻居的条目。

- **PIM SM 邻居表**

接口：	显示接口。
邻居：	此接口上学习到的相关邻居的信息。

存活时间： 邻居生成时间，表示该邻居条目自创建以来的存活时间。。

有效时间： 邻居的老化时间，表示还有多长时间邻居会被老化掉。

刷新： 点击此按钮来刷新邻居列表。

11.4.3 BSR

在一个 PIM SM 域内只能有一个 BSR，并由该 BSR 负责在整个 PIM SM 域内宣告 RP-Set 信息。BSR 是在众多候选 BSR 中通过竞争动态产生的。本页面用来配置候选 BSR 的相关参数，以及显示 BSR 和候选 BSR 的相关信息。

进入页面的方法：**组播路由>>PIM SM>>BSR**

图 11-24 BSR

条目介绍：

- **PIM SM 候选 BSR 配置**

接口： 选择需要配置候选 BSR 接口。

哈希掩码长度： 指定候选 BSR 的哈希掩码长度。

优先级： 指定候选 BSR 的优先级，默认值为 64。

- **PIM SM 已选举 BSR 信息**

BSR 地址： 显示选举出的 BSR 地址。

优先级： 显示选举出的 BSR 的优先级。

哈希掩码长度： 显示选举出的 BSR 的哈希掩码长度。

有限时间： 显示选举出的 BSR 的有效时间。

- **PIM SM 候选 BSR 信息**

  候选 BSR IP 地址： 显示候选 BSR 的 IP 地址。

  优先级： 显示候选 BSR 的优先级。

  哈希掩码长度： 显示候选 BSR 的哈希掩码长度。

11.4.4 RP

在 PIM SM 域中，RP 从组播源接收组播数据，并通过共享树向组播成员转发。在小型 PIM 网络中，RP 一般通过手工方式静态配置；在 PIM SM 域规模较大的大型网络中，一般需要通过自举机制来动态选举 RP。在本页面上可以进行静态 RP 和候选 RP 的相关配置。

进入页面的方法：**组播路由>>PIM SM>>RP**

图 11-25 RP 配置

条目介绍：

- **PIM SM 静态 RP 配置**

  RP 地址： 指定静态 RP 地址。

  覆盖： 配置覆盖模式。如果开启，不管候选 RP 是否配置，静态 RP 也会生效；如果关闭，静态 RP 只会在候选 RP 没有配置时生效。

- **PIM SM 候选 RP 配置**

  接口： 选择候选 RP 的接口。

  优先级： 指定候选 RP 的优先级。默认值为 192。

  间隔： 指定候选 RP 发送通告报文的间隔，单位为秒。默认值为 60 秒。

- **PIM SM 候选 RP 配置列表**

  接口： 显示候选 RP 的接口。

  优先级： 显示候选 RP 的优先级。

间隔： 显示候选 RP 发送通告报文的间隔。

下一个通告时间间隔： 显示下一个候选 RP 通告报文的发送时间。

11.4.5 RP 映射

每个组播组只能由唯一的一个 RP 为其转发数据。本页面显示组播组与 RP 的映射关系。

进入页面的方法：**组播路由>>PIM SM>>RP 映射**

图 11-26 RP 映射

条目介绍：

- **搜索选项**

全部： 显示所有的组播组到 RP 的映射关系。

组： 显示指定的组播组到 RP 的映射关系。

RP： 显示包含指定 RP 的映射条目。

- **组-RP 映射信息**

组： 显示组播组地址。

RP： 显示 RP 地址。

信息源： 显示发布 RP 信息的 BSR 地址。

优先级： 显示 RP 的优先级。

保持时间： 显示 RP 的保持时间。

有效时间： 显示 RP 的有效时间。如果 RP 是静态配置，则其有效时间为从不。

11.4.6 RP 信息

本页面显示每个组播组所选择的 RP。

进入页面的方法：**组播路由>>PIM SM>>RP 信息**

图 11-27 RP 信息

条目介绍：

- **搜索选项**

  全部： 显示所有的组播组到 RP 的映射关系。

  组： 显示指定的组播组到 RP 的映射关系。

  RP： 显示包含指定 RP 的映射条目。

- **RP 信息**

  组： 显示组播组地址。

  RP： 显示 RP 地址。

PIM SM 配置步骤：

步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，配置路由接口的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。
3	使能组播路由和 PIM SM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM SM>>PIM SM 接口配置**界面上使能接口的 PIM SM 功能。
4	配置静态 RP/ 配置候选 BSR 和候选 RP	必选操作。在**组播路由>>PIM SM>>RP** 页面上配置静态 RP；或者在**组播路由>>PIM SM>>RP** 页面上配置指定接口为候选 RP，并在**组播路由>>PIM SM>>BSR** 界面上配置指定接口为候选 BSR。
5	使能 IGMP	可选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能与组播接收者相连的路由接口的 IGMP 功能。

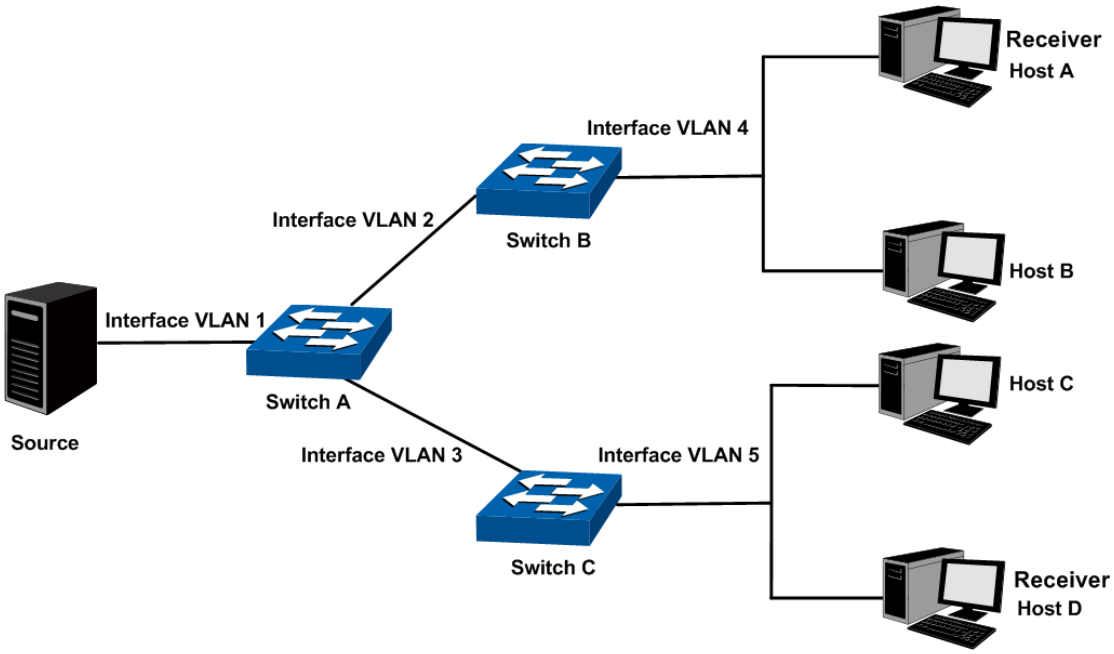
11.4.7 PIM SM 功能的组网应用

- **组网需求**

- 接收者通过组播来接收视频点播数据。整个网络中运行 PIM SM 作为组播路由协议。

- Host A 和 Host D 是组播接收者。
- 交换机 A 与交换机 B 通过 VLAN 接口 2 连接，交换机 A 与交换机 C 通过 VLAN 接口 3 连接。组播源服务器与交换机 A 通过 VLAN 接口 1 连接。
- Host A 与 Host B 通过 VLAN 接口 4 连接到交换机 B，Host C 与 Host D 通过 VLAN 接口 5 连接到交换机 C。
- 与 Host 相连的 VLAN 接口运行 IGMP 协议。
- 将交换机 A 的 VLAN 接口 1 配置为候选 BSR 和候选 RP。

➢ **组网图**



各交换机中每个 VLAN 接口的 IP 地址如下所示：

交换机 A：VLAN 接口 1: 192.168.1.2/24

VLAN 接口 2: 192.168.2.2/24

VLAN 接口 3: 192.168.3.2/24

交换机 B：VLAN 接口 2: 192.168.2.100/24

VLAN 接口 4: 192.168.4.100/24

交换机 C：VLAN 接口 3: 192.168.3.100/24

VLAN 接口 5: 192.168.5.100/24

➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，配置 VLAN 接口 1，2 和 3 的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。

步骤	操作	说明
3	使能组播路由和 PIM SM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM SM>>PIM SM 接口配置**界面上使能 VLAN 接口 1，2 和 3 的 PIM SM 功能。
4	配置候选 BSR 和候选 RP	必选操作。在**组播路由>>PIM SM>>BSR** 页面上配置 VLAN 接口 1 作为候选 BSR；在**组播路由>>PIM SM>>RP** 页面上配置 VLAN 接口 1 作为候选 RP。

- 配置交换机 B 和 C：

步骤	操作	说明
1	配置接口	必选操作。在**路由功能>>接口>>接口设置**页面，配置 VLAN 接口 3，4 和 5 的 IP 地址和子网掩码。
2	配置路由协议	必选操作。通过静态路由或者动态路由协议（如 OSPF 等）来配置路由条目，确保整个网络能互相通信，并通过单播路由协议来动态更新路由信息。
3	使能组播路由和 PIM SM	必选操作。在**组播路由>>全局配置>>全局配置**页面上使能组播路由；在**组播路由>>PIM SM>>PIM SM 接口配置**界面上使能 VLAN 接口 2，3，4 和 5 的 PIM SM 功能。
4	配置 IGMP	必选操作。在**组播路由>>IGMP 配置>>接口配置**页面上使能与组播接收者相连的 VLAN 接口 4 和 5 的 IGMP 功能。

11.5 静态组播配置

当组播的网络拓扑结构与单播网络拓扑结构相同时，接收者通过单播路由可以收到组播数据。然而组播的网络拓扑与单播网络拓扑有可能不同，而且网络中的一些路由器可能只支持单播而不支持组播。在这种情况下，可以通过配置静态组播路由为组播数据和单播数据提供不同的传输路径。需要注意以下两点：

- 静态组播路由的作用只在于影响 RPF 检查，而不能用于指导组播数据转发，故又称为 RPF 静态路由；
- 静态组播路由仅在所配置的组播路由器上生效，不会以任何方式被广播或者引入给其它路由器。

静态组播路由是 RPF 检查的重要依据。当配置了静态组播路由后，在进行 RPF 检查时，系统会同时查找单播路由表和静态组播路由表，从中分别选出最优单播路由和静态组播路由，通过比较以确定使用哪条作为 RPF 路由。

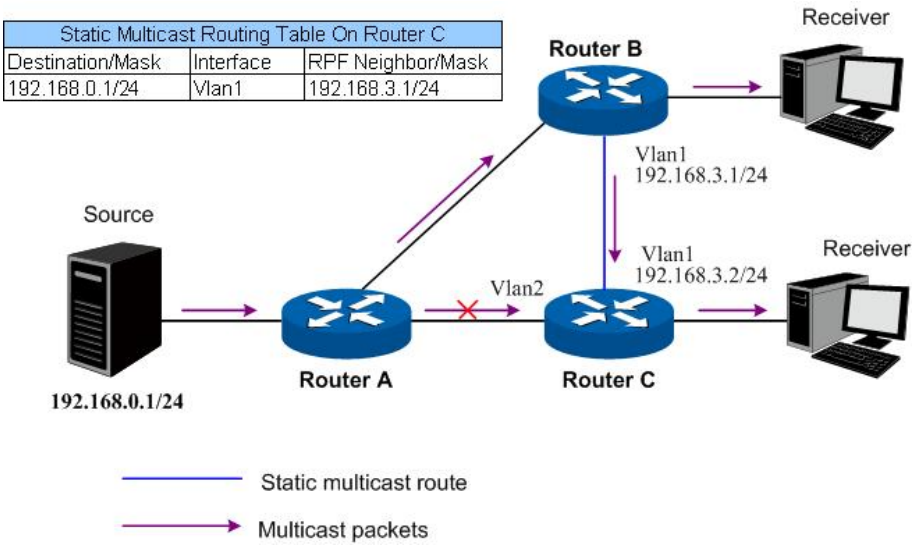


图 11-28 静态组播路由

如图 11-28 所示，当网络中没有配置静态组播路由时，Router C 到组播源（Source）的 RPF 邻居为 Router A，从 Source 发出的组播信息沿 Router A→Router C 的路径传输，与单播路径一致；当在 Router C 上配置了静态组播路由，指定从 Router C 到 Source 的 RPF 邻居为 Router B 后，从 Source 发出的组播信息将改变传输路径，沿 Router A→Router B→Router C 的路径传输。

本功能包括**静态组播配置**和**静态组播表**两个配置页面。

11.5.1 静态组播配置

静态组播条目需要管理员手动配置，不会随着网络拓扑的改变而自动改变。本页面可进行静态组播条目的配置及显示。

进入页面的方法：**组播路由>>静态组播配置>>静态组播配置**

图 11-29 静态组播配置

条目介绍：

- **静态组播配置**

源地址： 输入将要创建的静态组播条目的组播源地址。

源掩码： 输入与组播源匹配的子网掩码。

RPF 邻居： 输入通往组播源路径上的邻居路由的 IP 地址。

权值： 输入静态组播条目的管理权值，取值范围为 0-255，默认取值为 0，权值越小，优先级越高。

- **静态组播配置列表**

选择： 选择需要修改的静态组播条目。

源地址： 显示组播源地址。

源掩码： 显示组播源匹配的子网掩码。

RPF 邻居： 显示通往组播源路径上的邻居路由的 IP 地址。

权值： 显示静态组播条目的管理权值，取值范围为 0-255，默认取值为 0，权值越小，优先级越高。

11.5.2 静态组播表

本页面显示实际生效的静态组播条目。

进入页面的方法：**组播路由>>静态组播配置>>静态组播表**

图 11-30 静态组播表

条目介绍：

- **静态组播表**

源地址： 显示组播源地址。

源掩码： 显示组播源匹配的子网掩码。

RPF 邻居： 显示通往组播源路径上的邻居路由的 IP 地址。

权值： 显示静态组播条目的管理权值。权值越小，优先级越高。

回目录

第12章 服务质量

服务质量模块主要用于流量控制管理和优先级配置，针对各种网络应用的不同需求，为其提供不同的服务质量，对带宽资源进行最优配置，从而提供更高质量的网络服务体验，包括**QoS配置**、**流量管理**以及**语音VLAN**三个部分。

12.1 QoS配置

QoS（Quality of Service，即服务质量）功能用以提高网络传输的可靠性，并为您提供更高质量的网络服务体验。在传统的IP网络中，所有的报文都被无区别的等同对待，网络尽最大的努力（Best-Effort）发送报文，但对时延、可靠性等性能不能提供任何保证。伴随着网络技术、多媒体技术的飞速发展，IP网在现有的www，FTP，E-mail等服务的基础上，越来越多承载交互式多媒体通信业务如电视会议、远程教学、视频点播、可视电话等，而每种业务要求的传输时延、可变迟延、吞吐量和丢包率都不同。因此，为用户各种业务提供不同的服务质量（QoS）成为Internet发展的重要挑战。

通常所说的QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

- **QoS工作原理**

本交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来决定不同优先级队列的数据包被转发的方式，从而实现了QoS功能。

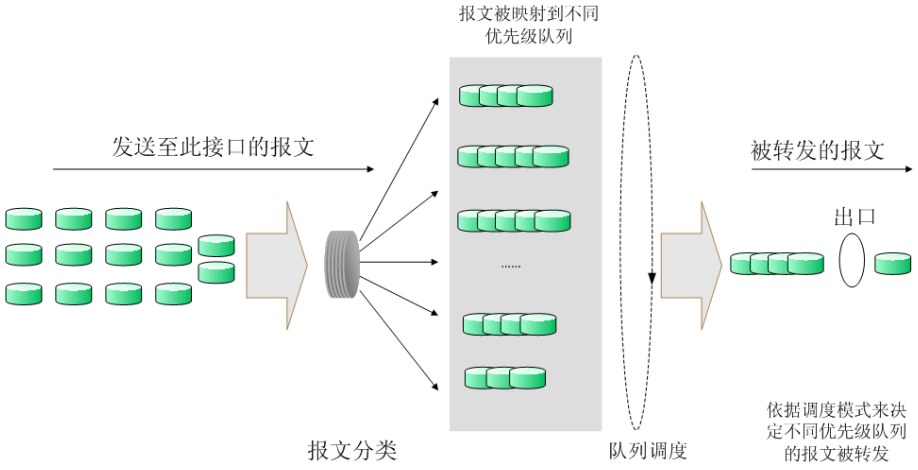


图 12-1 QoS工作原理

- 报文分类：依据一定的匹配规则识别出对象。
- 映射：用户可以根据优先级模式，将进入交换机的报文映射到不同的优先级队列中。本交换机提供三种优先级模式：基于端口的优先级、802.1P优先级和DSCP优先级。
- 队列调度：当网络拥塞时，必须解决多种数据流同时竞争使用资源的问题，通常采用队列调度加以解决。本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR模式和无优先级模式（Equ）。

➢ **优先级模式**

本交换机共有基于端口的优先级、IEEE 802.1P优先级和DSCP优先级三种模式。其中端口优先级和802.1P优先级是默认被启用的，DSCP优先级需配置使能。

1. 基于端口的优先级

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据入端口的CoS值以及802.1P中CoS到队列之间的映射关系来确定数据流的出口队列。

2. 802.1P优先级

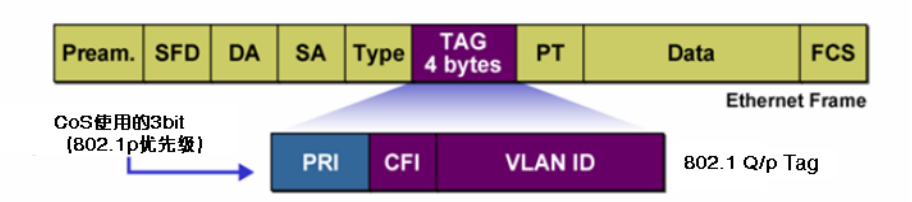


图 12-2 802.1Q的帧格式

如图所示，每一个802.1Q Tag中都有一个Pri域，该域由三个bit为组成，取值范围是0~7。802.1P优先级就是根据Pri的域值来决定数据帧的优先级。通过交换机的配置页面可配置不同的Pri域对应不同的优先级，交换机发送数据帧时，会根据数据帧的Tag决定发送的优先级。对于Untagged帧，交换机则按照该入口端口的默认优先级对数据帧进行QoS处理。

3. DSCP优先级

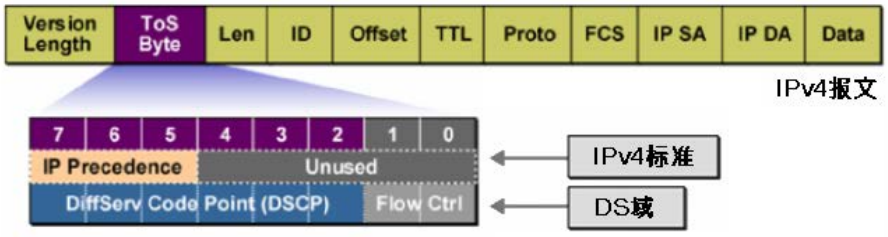


图 12-3 IP报文

如图所示，IP报文头部的ToS（Type of Service，服务类型）字段共有8bit，可以表征不同优先级特征的报文，前3个bit表示的是IP的优先级，取值范围是0~7。RFC2474重新定义了IP报文头部的ToS域，称之为DS域。其中DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前6个bit（0～5bit）表示，取值范围为0～63，后2个bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的DS字段对应不同的优先级，交换机转发报文时，将按照如下方式进行转发：

当没有启用DSCP优先级时，交换机根据数据包是否带有802.1Q Tag确定使用哪种优先级模式。对于带有Tag的数据包，应用802.1P优先级；否则应用端口优先级。当启用DSCP优先级时，如果接收的数据包是IP包，则应用DSCP优先级；对于非IP包，如果数据帧带有Tag则应用802.1P优先级，否则应用端口优先级。

➢ **调度模式**

在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。本交换机支持8个出口转发队列，TC0到TC7，其中TC0对应最低优先级的队列，TC7对应到最高优先级的队列。同时，本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR模式和无优先级模式（Equ）。

1. SP-Mode：严格优先级模式。SP模式的调度算法是交换机优先转发当前优先级最高的队列中的数据帧，等最高优先级队列转发完后，再转发次高级优先级队列。该调度模式的缺点是，在拥塞发生时，如果较高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

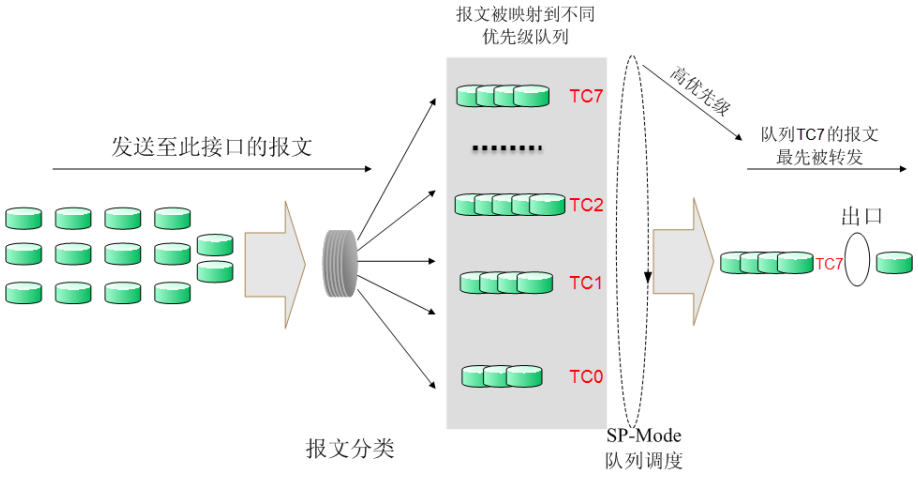


图 12-4 严格优先级模式

2. WRR-Mode：WRR优先级模式。WRR模式的调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间，加权值表示获取资源的比重。WRR队列避免了采用SP调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。TC0~TC7的默认权重比是1:2:4:8:16:32:64:128。

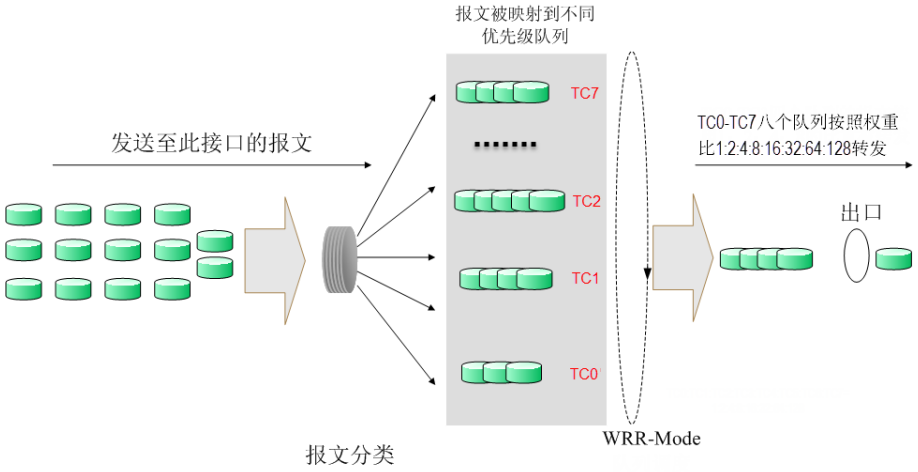


图 12-5 WRR优先级模式

3. SP+WRR-Mode：SP+WRR优先级模式，这种模式是前两种模式的混合。在这种模式下，交换机提供了两个调度组，分别是SP组和WRR组。其中SP组和WRR组之间遵循的是严格优先级调度规则，而WRR组内部队列遵循的是WRR调度模式。在该调度模式下TC7属于SP组；TC0~TC6属于WRR组，权重比是1:2:4:8:16:32:64。这样在调度的时候首先是TC7按照SP调度模式独自占用带宽，TC7数据转发完成后，TC0~TC6按照权重比占用带宽转发数据。
4. Equ-Mode：无优先级模式。这种模式下所有队列公平的占用带宽，实际上这是WRR模式的一种特殊情况，所有的队列权重比是1:1:1:1:1:1:1:1。

本交换机实现了基于端口、基于802.1P和基于DSCP的三种优先级模式定义，并提供八个队列调度模式来确定数据的转发优先级。QoS配置功能包括**端口配置**、**调度模式**、**802.1P**和**DSCP**四个配置页面。

12.1.1 端口配置

在端口配置页面中，您可以进行基于端口优先级的配置。

进入页面的方法：服务质量>>QoS配置>>端口配置

图 12-6 端口配置

条目介绍：

- **端口优先级配置**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选端口配置端口优先级，可多选。

端口： 显示交换机的物理端口。

优先级： 配置端口的所属CoS优先级等级。

LAG： 显示当前端口所属的LAG组。

配置步骤：

步骤	操作	说明
1	选择端口的优先级	必选操作。在**服务质量>>QoS配置>>端口配置**页面设置各端口的CoS优先级。
2	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS配置>>802.1P**页面的**优先级等级**表格中设置优先级与队列的映射关系。
3	选择调度模式	必选操作。进入**服务质量>>QoS配置>>调度模式**页面设置调度模式。

12.1.2 调度模式

在本页面可以进行交换机调度模式的选择。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以TC0,TC1…TC7表示不同的优先级队列。

进入页面的方法：服务质量>>QoS配置>>调度模式

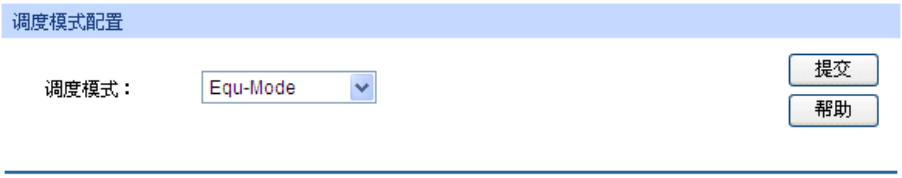


图 12-9 队列调度模式

条目介绍：

- **调度模式配置**

SP-Mode：	严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。
WRR-Mode：	加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0到TC7的权重比值是1:2:4:8:16:32:64:128。
SP+WRR-Mode：	SP+WRR模式，这种队列调度模式是SP和WRR模式的混合。在此模式下，交换机提供了SP和WRR两个调度组，TC7属于SP组；TC0~TC6属于WRR组，权重比是1:2:4:8:16:32:64。调度时，首先TC7按照SP模式独自占用带宽，然后是WRR组的成员TC0~TC6按照权重比共享带宽。
Equ-Mode：	无优先级模式。在此模式下所有队列公平的占用带宽，所有的队列权重比是1:1:1:1:1:1:1:1。

12.1.3 802.1P

在802.1P配置页面中，可以配置802.1P优先级。802.1P对802.1Q tag中的Pri字段与队列TC的映射关系进行了的定义，利用该字段的8个优先级等级将数据映射到不同的队列TC进行转发。交换机根据数据包是否带有802.1Q tag来确定所使用的优先级模式，对于带有tag的数据包，应用802.1P优先级，否则应用端口优先级。

进入页面的方法：服务质量>>QoS配置>>802.1P

图 12-8 802.1P/CoS映射

条目介绍：

- **tag与CoS到出口队列映射配置**

Tag-id/CoS-id： IEEE802.1P 协议里规定的或者是服务类型中8个优先级等级。

队列TC-id： 对应不同等级的优先级出口队列。以TC0、TC1 ... TC7表示。

配置步骤：

步骤	操作	说明
1	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS配置>>802.1P**页面中的**优先级等级**表格中设置优先级与队列的映射关系。
2	选择调度模式	必选操作。进入**服务质量>>QoS配置>>调度模式**页面设置调度模式。

12.1.4 DSCP

在DSCP映射配置页面中，可以进行DSCP优先级的配置。DSCP（DiffServ Code Point，区分服务编码点）是IEEE对IP ToS字段的重定义，利用该字段可以将IP报文划分为64个优先级。开启DSCP优先级后，如果转发的数据包是IP报文，则交换机应用DSCP优先级；对于非IP报文，交换机则根据802.1P优先级以及端口优先级转发。

进入页面的方法：服务质量>>QoS配置>>DSCP

图 12-7 DSCP映射

条目介绍：

- **优先级配置**

  DSCP优先级： 选择是否启用DSCP优先级。

- **优先级等级**

  DSCP： 根据IP包的DS域决定的优先级。优先级级别从0到63。

  优先级： 对应不同等级的CoS优先级。以CoS0、CoS1 ... CoS7表示。

配置步骤：

步骤	操作	说明
1	设置DSCP优先级与CoS优先级的映射关系	必选操作。在**服务质量>>QoS配置>>DSCP映射**页面启用DSCP优先级，设置DSCP优先级与CoS优先级的映射关系。
2	设置优先级与队列的映射关系	必选操作。在**服务质量>>QoS配置>>802.1P**页面的**优先级等级**表格中设置优先级与队列的映射关系。
3	选择调度模式	必选操作。进入**服务质量>>QoS配置>>调度模式**页面设置调度模式。

12.2 流量管理

流量管理用于限制交换机端口的带宽和广播流量，保证网络正常有效的运行，包括**带宽控制**和**风暴抑制**两个配置页面。

12.2.1 带宽控制

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

进入页面的方法：服务质量>>流量管理>>带宽控制

图 12-10 带宽控制

条目介绍：

- **带宽控制**

UNIT：	根据UNIT ID选择指定的交换机进行配置。
选择：	勾选端口以配置端口带宽，可多选也可不选。
入口带宽/出口带宽：	配置端口接收或转发数据时的带宽，从下拉列表选择或手动输入带宽参数。手动输入带宽参数后，系统将会自动选择与填写的数值最相近的64Kbps的整数倍值作为带宽的输入值。若选择“禁用”选项，则该端口的带宽控制会被取消，该端口的带宽限制将恢复为最大带宽。
LAG：	显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用广播风暴抑制，再启用入口带宽限制将使其失效。
- 在一个或多个端口上启用出口带宽限制时，建议将各端口的流量控制禁用，以保证交换机的正常工作。

12.2.2 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本交换机可以对三种常见的广播帧（广播包、组播包、UL包）进行限制。

进入页面的方法：服务质量>>流量管理>>风暴抑制

图 12-11 风暴抑制

条目介绍：

- **风暴抑制**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选端口以配置风暴抑制参数，可多选也可不选。

端口： 显示交换机的端口号。

广播包抑制(Kbps)： 配置端口的广播包抑制带宽，从下拉列表选择或手动输入带宽参数。手动输入带宽参数后，系统将会自动选择与填写的数值最相近的64Kbps的整数倍值作为带宽的输入值。若选择“禁用”选项，则该端口的广播包抑制功能会被取消。

组播包抑制(Kbps)： 配置端口的组播包抑制带宽，从下拉列表选择或手动输入带宽参数。手动输入带宽参数后，系统将会自动选择与填写的数值最相近的64Kbps的整数倍值作为带宽的输入值。若选择“禁用”选项，则该端口的组播包抑制功能会被取消。

UL包抑制(Kbps)： 配置端口的UL包抑制带宽，从下拉列表选择或手动输入带宽参数。手动输入带宽参数后，系统将会自动选择与填写的数值最相近的64Kbps的整数倍值作为带宽的输入值。若选择“禁用”选项，则该端口的UL包抑制功能会被取消。

LAG： 显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用入口带宽限制，再启用广播风暴抑制将使其失效。

12.3 语音VLAN

语音VLAN是为语音数据流而专门划分的VLAN。通过划分语音VLAN可以使语音数据自动被划分到语音VLAN中进行传输，便于对语音流进行有针对性的QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

- **语音数据流识别方法**

本交换机可以根据数据包中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到语音VLAN中传输。

OUI（Organizationally Unique Identifier）是MAC地址的前24位（二进制），是IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配全球唯一的标识符，从OUI地址可以判断出该设备的品牌。下表是常见语音设备商家产品的OUI地址，已在本交换机中设置为缺省OUI地址，设定不同的掩码可以调节交换机对MAC地址匹配的深度。

序号	OUI地址	设备商家
1	00-01-E3-00-00-00	Siemens phone
2	00-03-6B-00-00-00	Cisco phone
3	00-04-0D-00-00-00	Avaya phone
4	00-60-B9-00-00-00	Philips/NEC phone
5	00-D0-1E-00-00-00	Pingtel phone
6	00-E0-75-00-00-00	Polycom phone
7	00-E0-BB-00-00-00	3com phone

表 12-1 本交换机中缺省OUI地址

- **端口的语音VLAN模式**

端口的语音VLAN模式包括自动模式和手动模式，是指端口加入语音VLAN的方式。

自动模式：系统利用IP电话上电时发出的协议报文（UNTAG报文），通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将自动把语音报文的输入端口加入语音VLAN，配置报文的优先级。在设备上可以设置语音VLAN的老化时间。如果在老化时间内，系统没有从输入端口收到任何语音报文，系统将把该端口从语音VLAN中删除。端口的添加/删除过程由系统自动实现。

手动模式：需要手动把IP电话接入端口加入语音VLAN中，再通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将下发ACL规则、配置报文的优先级。

在实际应用中，端口模式需结合语音流形式和端口的链路类型进行设置，具体请参考下表。

端口模式	语音流类型	端口链路类型及处理方式
自动模式	TAG语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的默认VLAN不能是语音VLAN。
		GENERAL：支持，但接入端口的默认VLAN不能是语音VLAN，同时接入端口在语音VLAN中的出口规则必须为TAG。
	UNTAG语音流	所有链路类型端口都不支持处理。

端口模式	语音流类型	端口链路类型及处理方式
手动模式	TAG语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的默认VLAN不能是语音VLAN。
		GENERAL：支持，但接入端口的默认VLAN不能是语音VLAN，同时接入端口在语音VLAN中的出口规则必须为TAG。
	UNTAG语音流	ACCESS：支持。
		TRUNK：支持，且接入端口的默认VLAN必须是语音VLAN。
		GENERAL：支持，但接入端口的默认VLAN必须是语音VLAN，同时接入端口在语音VLAN中的出口规则必须为UNTAG。

表 12-2 端口模式与语音数据流的处理关系

注意：

- 如果语音设备发出的是TAG语音流，且接入的端口上使能了802.1X认证和Guest VLAN，为保证各种功能的正常使用，请为Voice VLAN、端口的默认VLAN和802.1X的Guest VLAN分配不同的VLAN ID。
- 如果语音设备发出的是UNTAG语音流，为实现Voice VLAN功能，只能将接入端口的默认VLAN配置为语音VLAN。

➢ **语音VLAN安全模式**

当端口使能了语音VLAN功能后，通过配置端口的安全模式还可以过滤数据流。若启用安全模式，则端口只转发语音数据包，对于其它源MAC地址不匹配OUI地址的数据包，端口将直接丢弃。若禁用安全模式，则端口转发所有数据包。

安全模式	报文类型	处理方式
启用	UNTAG报文	当该报文源MAC地址是可识别的OUI地址时，允许该报文在语音VLAN内传输，否则将该报文丢弃。
	带有语音VLAN TAG的报文	
	带有其它VLAN TAG的报文	根据指定端口是否允许该VLAN通过来对报文进行转发和丢弃的处理，不受语音VLAN安全模式的影响。
禁用	UNTAG报文	不对报文的源MAC地址进行检查，所有报文均可在语音VLAN内传输。
	带有语音VLAN TAG的报文	
	带有其它VLAN TAG的报文	根据指定端口是否允许该VLAN通过来对报文进行转发和丢弃的处理，不受语音VLAN安全模式的影响。

表 12-3 安全模式与各种数据的处理关系

注意：

- 除非有特殊需求，请不要在语音VLAN中同时传输语音和其它业务数据。

12.3.1 全局配置

在全局配置页面中，可以设置语音VLAN的全局参数。

进入页面的方法：服务质量>>语音VLAN>>全局配置

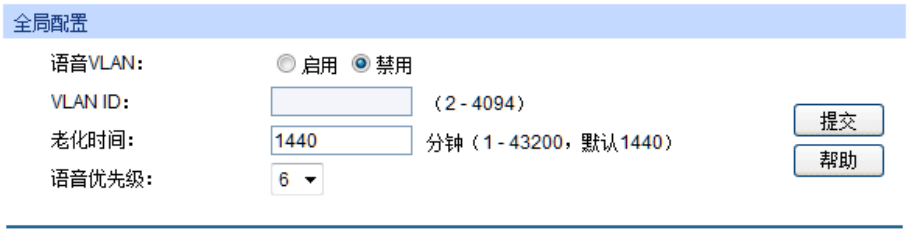


图 12-12 语音VLAN全局配置

条目介绍：

- **全局配置**

语音VLAN：	选择是否启用语音VLAN功能。
VLAN ID：	输入该语音VLAN的VLAN ID。
老化时间：	设置自动模式下的端口成员在OUI地址老化后的存活时间。
语音优先级：	设置语音VLAN数据包的802.1P优先级。

12.3.2 端口配置

在启用语音VLAN功能之前，需要在端口配置页面中配置各端口的功能参数。

进入页面的方法：服务质量>>语音VLAN>>端口配置

图 12-13 语音VLAN端口配置

注意：

- 若LAG组成员端口要启用语音VLAN功能，请保持端口的成员模式和端口模式一致。
- 当端口为语音VLAN的成员端口时，修改该端口的成员模式为“自动”，此端口首先会退出语音VLAN，直到收到语音数据时再自动加入语音VLAN。

条目介绍：

- **端口配置**

UNIT：	根据UNIT ID选择指定的交换机进行配置。
选择：	勾选端口配置端口的语音VLAN参数，可多选。
端口：	显示交换机的端口号。
成员模式：	设置端口加入语音VLAN的方式，有手动和自动两种方式。 ● 自动：交换机根据端口是否收到语音数据自动维护端口加入或退出语音VLAN。 ● 手动：请根据需要手动设置端口加入或退出语音VLAN。
安全模式：	设置端口转发数据包的模式。 ● 禁用：端口转发所有数据。 ● 启用：端口只转发语音数据。
成员状态：	显示端口当前在语音VLAN中的状态。
LAG：	显示端口当前所属的汇聚组。

12.3.3 OUI配置

本交换机支持新建OUI条目，将特殊语音设备的MAC地址添加到交换机支持的OUI信息中，并以此OUI地址判断数据是否是语音数据。当交换机接收到数据包时，将分析数据包并判断是否是语音数据，如果是语音数据则将该端口自动添加到语音VLAN中。

进入页面的方法：服务质量>>语音VLAN>>OUI配置

图 12-14 语音VLAN OUI配置

条目介绍：

- **新建条目**

OUI地址：	输入语音设备的OUI地址。
OUI掩码：	选择OUI地址掩码，常见为FF-FF-FF-00-00-00。

OUI描述： 对此OUI进行描述，以便区分不同VoIP设备。

- **OUI列表**

OUI地址： 显示语音设备的OUI地址。

OUI掩码： 显示语音设备的OUI地址掩码。

OUI描述： 显示此OUI的描述信息。

语音VLAN配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型，并根据表 12-2设置语音设备连接端口的端口类型。
2	创建VLAN	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，请输入VLAN ID并对其进行描述，在此页面中请同时勾选VLAN包含的端口。
3	添加OUI地址	可选操作。在**服务质量>>语音VLAN>>OUI配置**页面中的查看交换机是否支持相应的OUI模板，若不支持请在此页面中添加。
4	使能端口语音VLAN特性	必选操作。在**服务质量>>语音VLAN>>端口配置**页面设置语音VLAN中各端口的功能参数。
5	使能语音VLAN	必选操作。在**服务质量>>语音VLAN>>全局配置**页面中使能语音VLAN功能，并设置全局参数。

回目录

第13章 访问控制

随着网络规模的扩大以及流量的增加，如何有效地控制网络安全和分配带宽已成为网络管理的重要内容。ACL（Access Control List，访问控制列表）功能，通过配置报文的匹配规则和处理方式来实现对数据包的过滤功能，从而有效防止非法用户对网络的访问。另外ACL功能也可以控制流量，节约网络资源。ACL功能对网络安全的控制提供了很大的方便。

在本交换机中，ACL功能可以对数据包的L2-L4层的协议字段进行匹配。通过定义时间段可以设置ACL规则的生效时间，配置policy可以对匹配了ACL规则的数据包进行处理。

13.1 时间段配置

当用户配置的ACL规则需要在特定时间段生效时，可以先配置时间段，然后设置ACL规则直接引用该时间段即可。ACL规则只在指定的时间段内生效，从而实现基于时间段的ACL过滤。

本交换机可设置的时间段包括绝对时间、周期时间和节假日。绝对时间可以设置在自然日内的生效日期，周期时间则可以设置在每周的固定工作日生效，同时可以根据需要设置节假日来应对某些特殊意义的日期。在每个时间段内，还可以设置四个小的时间片段使生效时间更灵活。

本功能包括**时间段列表**、**新建时间段**和**节假日定义**三个配置页面。

13.1.1 时间段列表

在时间段列表页面，可以查看和编辑当前已添加的时间段信息。

进入页面的方法：访问控制>>时间段配置>>时间段列表

图 13-1 查看时间段列表

条目介绍：

- **时间段列表**

  选择： 选择时间段条目进行删除。

  序号： 显示时间段条目的序号。

  时间段名称： 显示时间段的名称。

  时间片段： 显示时间段中的时间片段。

  应用模式： 显示时间段的应用模式。

  操作： 点击相应按键可以查看或编辑相应时间段的详细配置信息。

13.1.2 新建时间段

在新建时间段页面，可以添加时间段信息。

进入页面的方法：访问控制>>时间段配置>>新建时间段

图 13-2 创建时间段

条目介绍：

- **时间段定义**

  时间段名称： 填写时间段的名称，便于区分各个时间段的信息。

  节假日： 配置时间段的节假日模式。只有当系统日期在节假日内时，基于该时间段的ACL规则才能生效。

  绝对时间： 配置时间段的绝对时间模式。只有当系统日期在绝对时间内，基于该时间段的ACL规则才能生效。

  周期： 配置时间段的周期模式。只有当系统日期在周期时间内，基于该时间段的ACL规则才能生效。

- **时间片段**

  起始时间： 配置时间段中时间片段的起始时间。

  结束时间： 配置时间段中时间片段的结束时间。

- **时间片段列表**

  序号： 显示时间片段的序号。

  起始时间： 显示时间段中时间片段的起始时间。

  结束时间： 显示时间段中时间片段的结束时间。

  操作： 点击删除即可删除相应的时间片段。

13.1.3 节假日定义

节假日定义可以提供与工作日不同的安全访问控制策略。在本页面，可以根据工作安排自行定义节假日。

进入页面的方法：访问控制>>时间段配置>>节假日定义

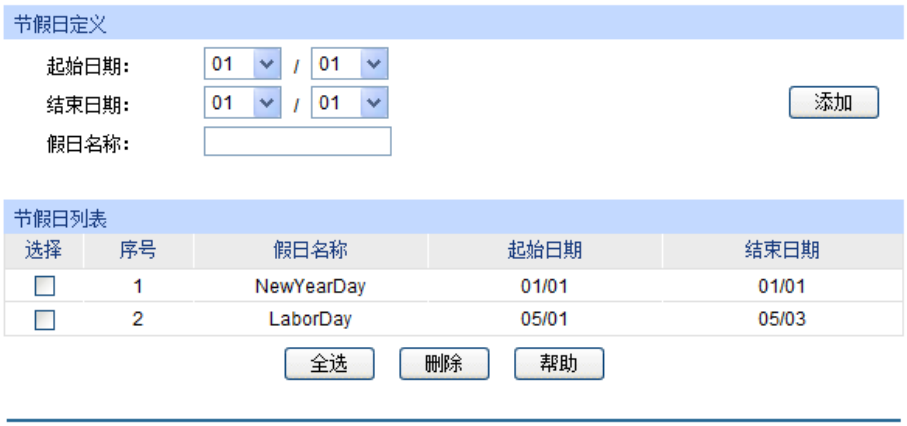


图 13-3 节假日定义

条目介绍：

- **节假日定义**

  起始日期： 配置节假日起始日期。

  终止日期： 配置节假日终止日期。

  假日名称： 填写假日名称，请输入英文字符。

- **节假日列表**

  选择： 选择节假日条目进行删除。

  序号： 显示节假日条目的序号。

  假日名称： 显示节假日名称。

  起始日期： 显示节假日起始日期。

  终止日期： 显示节假日终止日期。

13.2 ACL配置

在ACL功能中，一个ACL可以包括多个规则，而每个规则可以针对数据包中特定字段内容进行匹配。在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，交换机将对该报文执行第一次匹配的规则指定的动作，以此来提高交换机的效率。

ACL配置功能包括**ACL列表**、**新建ACL**、**MAC ACL**、**标准IP ACL**和**扩展IP ACL**五个配置页面。

13.2.1 ACL列表

在ACL列表页面，可以查看交换机中当前已配置的ACL详细信息。

进入页面的方法：访问控制>>ACL配置>>ACL列表

图 13-4 查看ACL列表

条目介绍：

- **ACL显示**

  选择ACL： 选择已创建的ACL。

  ACL类型： 显示该ACL的类型。

  规则排序： 显示该ACL内部的规则如何排序。

- **规则列表**

此处可以查看或编辑ACL内部的详细规则信息，点击条目的操作按键可以对规则条目进行排序。

13.2.2 新建ACL

在新建ACL页面，可以创建ACL。

进入页面的方法：访问控制>>ACL配置>>新建ACL

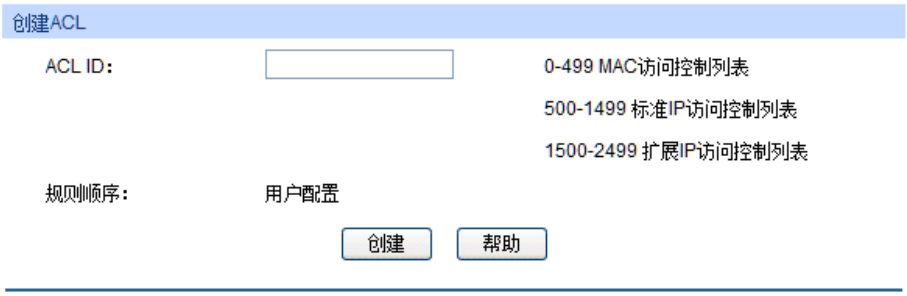


图 13-5 创建ACL

条目介绍：

- **创建ACL**

  ACL ID： 配置ACL ID。

  规则排序： 配置该ACL内部的规则如何排序。默认为用户配置。

  用户配置：按照用户配置规则的先后顺序进行规则匹配。

13.2.3 MAC ACL

MAC ACL根据数据包的源MAC地址、目的MAC地址、VLAN、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL配置>>MAC ACL

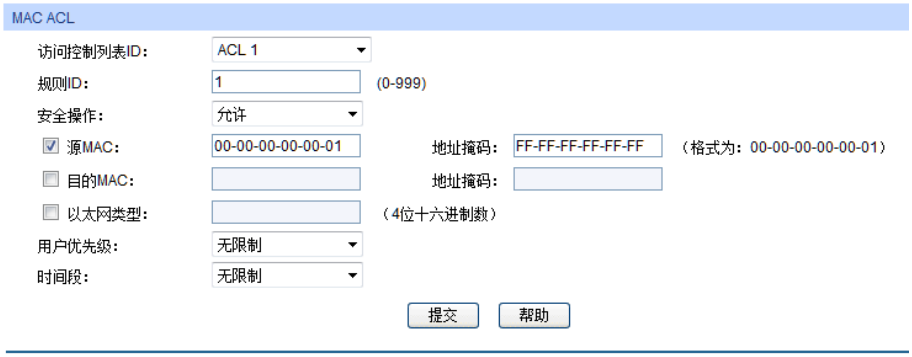


图 13-6 为MAC ACL添加规则

条目介绍：

- **MAC ACL**

访问控制列表ID： 选择需要配置的ACL ID。

规则ID： 填写规则ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。

- 允许：转发数据包。
- 丢弃：丢弃数据包。

源MAC： 填写规则包含的源MAC地址信息。

目的MAC： 填写规则包含的目的MAC地址信息。

地址掩码： 填写MAC地址掩码，掩码置1表示严格匹配。

以太网类型： 配置规则包含的以太网类型信息。

用户优先级： 选择该规则对数据包的tag优先级字段的匹配要求。默认为无限制。

时间段： 选择规则生效的时间段名称。默认为无限制。

13.2.4 标准IP ACL

标准IP ACL可以根据数据包的IP地址信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL配置>>标准IP ACL

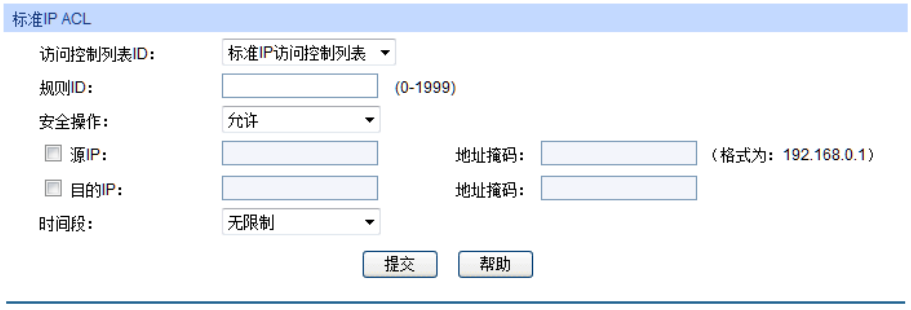


图 13-7 为标准IP ACL添加规则

条目介绍：

- **标准IP ACL**

访问控制列表ID：	选择需要配置的ACL ID。
规则ID：	填写规则ID。
安全操作：	选择交换机对满足匹配规则的数据包的处理方式。默认为允许。 ● 允许：转发数据包。 ● 丢弃：丢弃数据包。
源IP：	填写规则包含的源IP地址信息。
目的IP：	填写规则包含的目的IP地址信息。
地址掩码：	填写IP地址掩码，掩码置1表示严格匹配。
时间段：	选择规则生效的时间段名称。

13.2.5 扩展IP ACL

扩展IP ACL可以根据报文的源IP地址信息、目的IP地址信息、IP承载的协议类型、协议的特性等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL配置>>扩展IP ACL

图 13-8 为扩展IP ACL添加规则

条目介绍：

- **扩展IP ACL**

访问控制列表ID：	选择需要配置的ACL ID。
规则ID：	填写规则ID。
安全操作：	选择交换机对满足匹配规则的数据包的处理方式。默认为允许。 ● 允许：转发数据包。 ● 丢弃：丢弃数据包。

源IP：	填写规则包含的源IP地址信息。
目的IP：	填写规则包含的目的IP地址信息。
地址掩码：	填写IP地址掩码，掩码置1表示严格匹配。
IP协议：	选择规则包含的IP协议信息。
TCP Flag：	当IP协议选择TCP时，此处配置Flag匹配条件。
源端口号：	当IP协议选择TCP/UDP时，此处配置规则包含的TCP/UDP源端口。
目的端口号：	当IP协议选择TCP/UDP时，此处配置规则包含的TCP/UDP目的端口。
DSCP：	填写规则包含的DSCP域信息。
IP ToS/IP Pre	填写规则包含的IP ToS或IP Pre域信息
时间段：	选择规则生效的时间段名称。

13.3 Policy配置

Policy功能是将ACL规则和处理方式组合起来，组成一个访问控制策略，对符合相应ACL规则的数据包进行控制，处理方式包括流镜像、流监控和端口重定向。

Policy配置功能包括**Policy列表**、**新建Policy**、**配置Policy**三个配置页面。

13.3.1 Policy列表

在Policy页面可以查看和编辑ACL规则的数据处理方式。

进入页面的方法：访问控制>>Policy配置>>Policy列表

图 13-9 查看Policy列表

条目介绍：

- **Policy显示**

选择Policy：	选择需要查看的policy名称。

- **Action列表**

选择：	选择动作条目进行删除。
序号：	显示动作条目的序号。
ACL ID：	显示此Policy中包含的ACL。
流镜像：	显示此Policy中的流镜像端口。
流监管：	显示该Policy中添加的流监管动作信息。
端口重定向：	显示该Policy中添加的端口重定向动作信息。
QoS重标记：	显示该Policy中添加的QoS重标记动作信息。

操作： 点击<编辑>按键，可以对编辑相应的policy条目。

13.3.2 新建Policy

在此页面中可以创建Policy。

进入页面的方法：访问控制>>Policy配置>>新建Policy

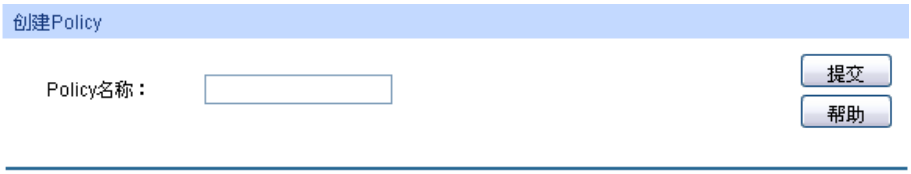


图 13-10 创建Policy

条目介绍：

- **创建Policy**

Policy名称： 填写Policy的名称。

13.3.3 配置Policy

在此页面中，可以配置Policy对应的ACL规则以及包含的动作，此动作是对匹配了相应ACL规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy配置>>Policy设置

图 13-11 为Policy添加ACL并设置动作

条目介绍：

- **Policy设置**

选择Policy： 选择Policy的名称。

选择ACL： 选择ACL作为Policy作用的对象。

流镜像： 配置该Policy的数据包执行流镜像动作，镜像到选定的端口。

流监管： 配置该Policy的数据包执行流限速动作。

- 额定速率：为匹配了相应ACL的数据包配置额定转发速率。
- 超速处理：为超过额定速率的数据包选择处理方式。

端口重定向： 配置该Policy的数据包执行端口重定向动作，改变转发端口。

- 指定出口端口：将匹配了相应ACL的数据包指定到固定端口转发。

QoS重标记： 配置该Policy的数据包执行QoS重标记动作，以新的QoS标识进行转发。

- DSCP：将匹配了相应ACL的数据包的DSCP域修改成设定值。
- 本地优先级：为匹配了相应ACL的数据包设定本地优先级，将其列入具体的转发队列进行转发。

13.4 绑定配置

只有将Policy和端口/VLAN绑定，Policy才能生效；将Policy与端口/VLAN进行绑定后，端口和VLAN会对接收到的数据包根据Policy进行匹配处理。绑定配置功能将Policy应用到某个端口或者VLAN上。

绑定配置功能包括**显示绑定、端口绑定、VLAN绑定**三个配置页面。

13.4.1 绑定列表

在此页面中可以查看已进行端口/VLAN绑定的Policy条目。

进入页面的方法：访问控制>>绑定配置>>绑定列表

图 13-12 查看Policy与端口/VLAN绑定信息

条目介绍：

- **选择显示模式**

选择显示模式： 请根据需要选择参考已绑定的条目类别。

- **Policy绑定列表**

选择： 选择绑定条目进行删除。

序号： 显示绑定条目的序号。

Policy名称： 显示绑定的Policy名称。

绑定接口： 显示与相应Policy绑定的端口号或VID。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

13.4.2 端口绑定

在此页面中可以将Policy与端口进行绑定。

进入页面的方法：访问控制>>绑定配置>>端口绑定

图 13-13 将Policy与端口进行绑定

条目介绍：

- **端口绑定配置**

Policy名称： 选择需要绑定的Policy名称。

端口： 在端口选择区根据UNIT ID点选指定交换机的具体端口。

- **端口绑定列表**

序号： 显示绑定条目的序号。

Policy名称： 显示绑定的Policy名称。

端口： 显示与相应Policy绑定的端口号。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

13.4.3 VLAN绑定

在此页面中可以将Policy与VLAN进行绑定。

进入页面的方法：访问控制>>绑定配置>>VLAN绑定

图 13-14 将Policy与VLAN进行绑定

条目介绍：

- **VLAN绑定配置**

Policy名称： 选择需要绑定的Policy名称。

VLAN ID： 填写需要绑定的已建立的VLAN ID。

- **VLAN绑定列表**

序号： 显示绑定条目的序号。

Policy名称： 显示绑定的Policy名称。

VLAN ID： 显示与相应Policy绑定的VLAN ID。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

配置步骤：

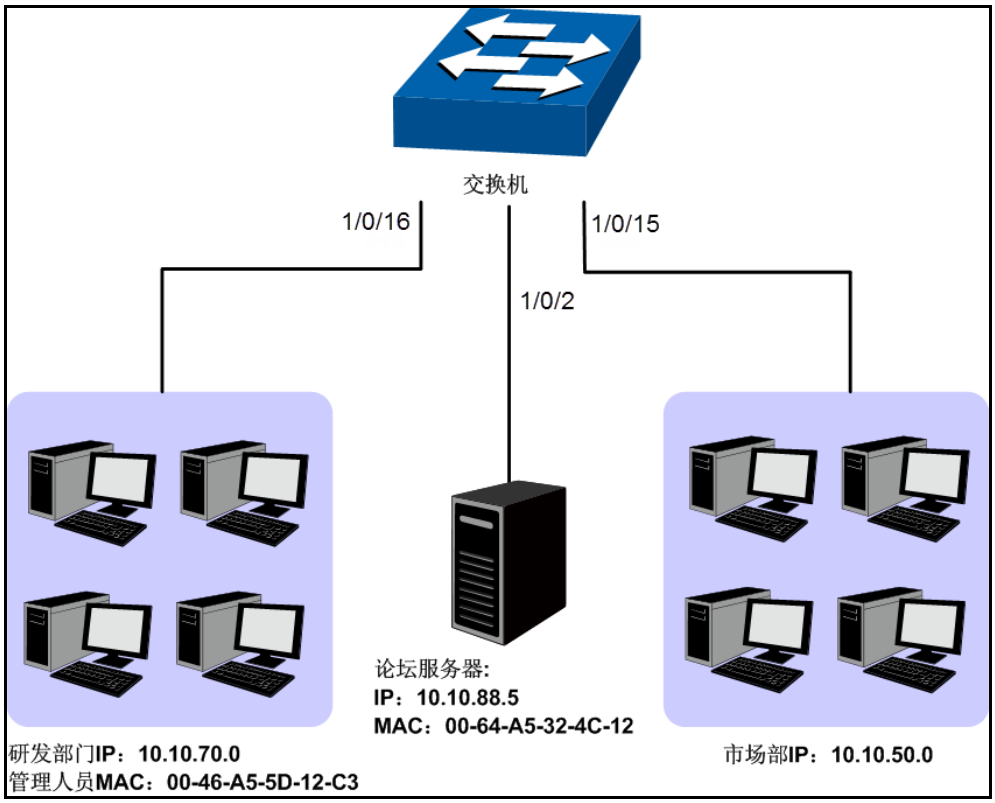
步骤	操作	说明
1	设置生效时间段	必选操作。在**访问控制>>时间段配置**三个标签页中配置ACL规则的生效时间段。
2	配置ACL规则	必选操作。在**访问控制>>ACL配置**三个标签页中配置ACL规则对数据包进行匹配。
3	配置Policy	必选操作。在**访问控制>>Policy配置**三个标签页中配置Policy，对匹配了相应ACL规则的数据包，可以通过Policy设置处理方式。
4	将Policy与端口/VLAN绑定	必选操作。在**访问控制>>绑定配置**三个标签页中将Policy与端口/VLAN进行绑定，将Policy应用到相应的端口/VLAN上。

13.5 访问控制功能组网应用

- **组网需求**

1. 研发部门的管理人员自由访问公司论坛，管理人员MAC地址为00-46-A5-5D-12-C3。
2. 研发部门工作人员在工作时间可以访问公司论坛。
3. 市场部人员在工作时间不能访问公司论坛。
4. 市场部和研发部门之间互相不能访问。

- 组网图



- 配置步骤

步骤	操作	说明
1	配置时间段	在**访问控制>>时间段配置**功能处，新建时间段，描述为work_time，时间段采用周期时间，周期时间选择工作日周一到周五，时间片段添加08:00~18:00。
2	需求1配置	在**访问控制>>ACL配置>>新建ACL**页面，创建ACL 11。 在**访问控制>>ACL配置>>MAC ACL**页面，选择ACL 11，创建规则1，安全操作设置为允许；勾选源MAC设置为00-46-A5-5D-12-C3，掩码为FF-FF-FF-FF-FF-FF；时间段选择无限制。 在**访问控制>>Policy配置>>新建Policy**页面，创建Policy，名称定为manager。 在**访问控制>>Policy配置>>配置Policy**页面，将ACL 11应用到Policy manager。 在**访问控制>>绑定配置>>端口绑定**页面，选择Policy manager与端口1/0/16绑定。

步骤	操作	说明
3	需求2、4配置	在**访问控制>>ACL配置>>新建ACL**页面，创建ACL 500。 在**访问控制>>ACL配置>>标准IP ACL**页面，选择ACL 500，创建规则1，安全操作设置为丢弃；设置源IP为10.10.70.0，掩码为255.255.255.0；设置目的IP为10.10.50.0，掩码为255.255.255.0；时间段选择无限制。 在**访问控制>>ACL配置>>标准IP ACL**页面，选择ACL 500，创建规则2，安全操作设置为允许；设置源IP为10.10.70.0，掩码为255.255.255.0；设置目的IP为10.10.88.5，掩码为255.255.255.255；时间段选择work_time。 在**访问控制>>ACL配置>>标准IP ACL**页面，选择ACL 500，创建规则3，安全操作设置为丢弃；设置源IP为10.10.70.0，掩码为255.255.255.0；设置目的IP为10.10.88.5，掩码为255.255.255.255；时间段选择无限制。 在**访问控制>>Policy配置>>新建Policy**页面，创建Policy，名称定为limit1。 在**访问控制>>Policy配置>>配置Policy**页面，将ACL 500应用到Policy limit1。 在**访问控制>>绑定配置>>端口绑定**页面，选择Policy limit1与端口1/0/16绑定。
4	需求3、4配置	在**访问控制>>ACL配置>>新建ACL**页面，创建ACL 501。 在**访问控制>>ACL配置>>标准IP ACL**页面，选择ACL 501，创建规则4，安全操作设置为丢弃；设置源IP为10.10.50.0，掩码为255.255.255.0；设置目的IP为10.10.70.0，掩码为255.255.255.0；时间段选择无限制。 在**访问控制>>ACL配置>>标准IP ACL**页面，选择ACL 501，创建规则5，安全操作设置为丢弃；设置源IP为10.10.50.0，掩码为255.255.255.0；设置目的IP为10.10.88.5，掩码为255.255.255.255；时间段选择work_time。 在**访问控制>>Policy配置>>新建Policy**页面，创建Policy，名称定为limit2。 在**访问控制>>Policy配置>>配置Policy**页面，将ACL 501应用到Policy limit2。 在**访问控制>>绑定配置>>端口绑定**页面，选择Policy limit2与端口1/0/15绑定。

回目录

第14章 网络安全

网络安全模块为保护局域网安全提供了多项安全措施，包括**四元绑定**、**DHCP侦听**、**ARP防护**、**IP源防护**、**DoS防护**以及**802.1X认证**六个部分，请根据实际需要进行配置。

14.1 四元绑定

四元绑定，是将计算机的MAC地址、IP地址、所属VLAN以及与之相连的交换机的端口号四者绑定，以下这四个参数信息简称四元信息。该功能可以启用ARP防护和IP源防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种四元绑定方式：

1) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

2) 扫描绑定：通过ARP扫描获取局域网用户的四元信息，并根据实际需要选择扫描结果进行绑定。此绑定方式只需在相应的功能页面输入IP地址段进行扫描。

3) DHCP侦听：通过DHCP侦听功能侦听DHCP广播包，记录数据包中的IP、MAC和VLAN ID等信息。当局域网中搭建了DHCP服务器给局域网用户分配IP地址时，DHCP侦听功能可以很方便地记录局域网用户的四元信息。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是扫描绑定，DHCP侦听优先级最低。

本功能包括**绑定列表**、**手动绑定**和**扫描绑定**三个配置页面。

14.1.1 绑定列表

在绑定列表页面中，可以查看当前交换机已进行四元绑定的局域网计算机条目信息。

进入页面的方法：网络安全>>四元绑定>>绑定列表

图 14-1 查看四元绑定信息

条目介绍：

- **搜索条目**

来源： 选择查看不同来源的四元绑定条目。

- 全部来源：查看全部四元绑定条目。
- 手动添加：只查看手动添加的四元绑定条目。
- ARP扫描：只查看通过ARP扫描获得的四元绑定条目。
- DHCP侦听：只查看通过DHCP侦听获得的四元绑定条目。

IP： 根据IP地址搜索具体的四元绑定条目。输入IP地址后点击<选择>按键进行快速搜索。

- **四元绑定表**

选择： 勾选条目可修改主机名及防护范围，可多选。

主机名： 显示主机描述名称。

IP地址： 显示主机IP地址。

MAC地址： 显示主机MAC地址。

VLAN ID： 显示VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示并编辑此条目支持的防护范围，可以进行ARP防护和IP源防护两种，也可以同时启用两种防护。

来源： 显示此条目的来源。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于MSTP等功能造成的。
- 严重：已确定的冲突条目。

注意：

- 冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。
- 多条“来源”优先级相同的条目中只有最后添加/修改的条目生效。

14.1.2 手动绑定

当已经获取了局域网用户的四元信息时，可以将四元信息静态绑定。

进入页面的方法：网络安全>>四元绑定>>手动绑定

图 14-2 手动绑定四元信息

条目介绍：

- **手动绑定**

主机名： 输入主机描述名称。

IP地址： 输入主机IP地址。

MAC地址： 输入主机MAC地址。

VLAN ID： 输入VLAN ID。

防护范围： 选择此条目支持的防护范围，可以进行ARP防护和IP源防护两种，也可以同时启用两种防护。

端口： 在端口选择区根据UNIT ID点选指定交换机的端口。

绑定： 点击此按键将上述输入信息进行绑定。

- **手动绑定条目**

UNIT： 根据UNIT ID选择查看指定交换机上的手动绑定列表。

选择： 勾选条目进行删除。

主机名： 显示主机描述名称。

IP地址： 显示主机IP地址。

MAC地址： 显示主机MAC地址。

VLAN ID： 显示VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围。

冲突：	显示此绑定条目与其它条目的冲突状态。 ● 警告：表示此条目冲突可能是由于MSTP等功能造成的。 ● 严重：已确定的冲突条目。

14.1.3 扫描绑定

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的IP地址解析为数据链路层地址。IP地址只是主机在网络层中的地址，如果要将网络层中数据包传送给目的主机，必须知道目的主机的数据链路层地址（比如以太网络MAC地址）。因此必须将IP地址解析为数据链路层地址。

ARP协议用于将IP地址解析为MAC地址，并在主机内部维护一张ARP表，记录最近与本主机通信的其它主机的MAC地址与IP地址的对应关系。当主机需要与陌生主机通信时，首先进行ARP地址解析，ARP地址解析过程如图 14-3所示：

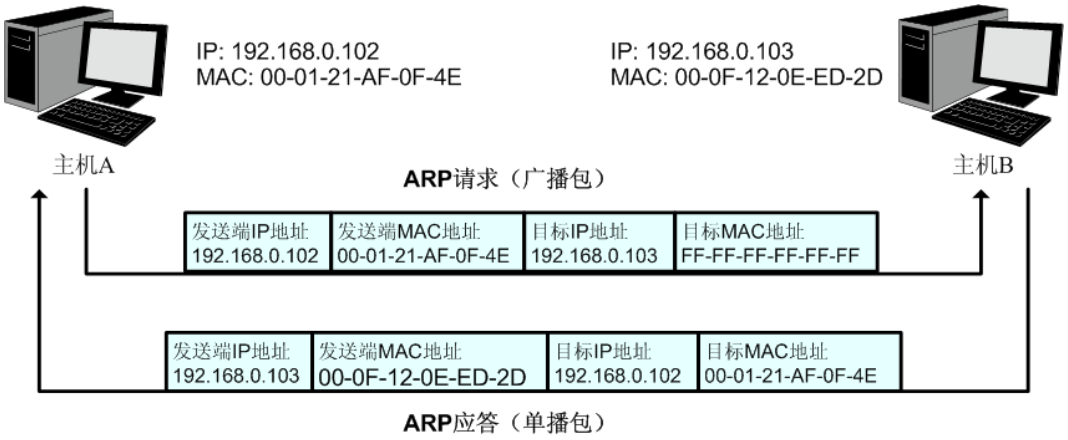


图 14-3 ARP地址解析图

1) A在自己的ARP表中查询是否存在主机B的IP地址和MAC地址的对应条目。若存在，直接向主机B发送数据。若不存在，则A向整个局域网中广播一份称为“ARP请求”的数据链路帧，这个请求包含发送端（即主机A）的IP地址和MAC地址以及接收端（即主机B）的IP地址。

2) 局域网的每个主机接收到主机A广播的ARP请求后，目的主机B识别出这是发送端在询问它的IP地址，于是给主机A发出一个ARP应答。这个应答包含了主机B的MAC地址。

3) 主机A接收到主机B发出的ARP应答后，就将主机B的IP地址与MAC地址的对应条目添加自己的ARP表中，以便后续报文的转发。

扫描绑定功能即通过交换机向局域网或VLAN发送指定IP段的ARP请求报文，当收到相应的ARP应答报文时，将分析ARP应答报文来获得四元信息。由此可见，通过扫描绑定功能可以很方便的将局域网用户的四元信息进行绑定。

进入页面的方法：网络安全>>四元绑定>>扫描绑定

图 14-4 扫描绑定四元信息

条目介绍：

- **ARP扫描**

起始IP地址：	输入起始IP地址。
结束IP地址：	输入结束IP地址。
VLAN ID:	输入VLAN ID，在相应的VLAN中进行扫描。若留空，则发送untag数据包进行扫描。
扫描：	点击<扫描>按键将对局域网计算机进行扫描。

- **扫描结果**

UNIT：	根据UNIT ID选择查看指定交换机上的扫描结果。
选择：	勾选条目进行绑定或删除。
主机名：	显示主机描述名称或对主机进行描述以便区分。
IP地址：	显示主机IP地址。
MAC地址：	显示主机MAC地址。
VLAN ID：	显示VLAN ID。
端口：	显示主机连接的交换机端口。
防护范围：	显示此条目支持的防护范围或者对此条目开启防护功能。
冲突：	显示此绑定条目与其它条目的冲突状态。 ● 警告：表示此条目冲突可能是由于MSTP等功能造成的。 ● 严重：已确定的冲突条目。

14.2 DHCP 侦听

随着网络规模的不断扩大和网络复杂度的提高，经常出现计算机的数量超过可供分配的IP地址的情况。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的IP地址也必须经常更新，从而导致网络配置越来越复杂。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在BOOTP协议基础上进行了优化和扩展而产生的一种网络配置协议，并有效解决了上面这些问题。

- **DHCP工作原理**

DHCP采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等配置信息，以实现网络资源的动态配置。通常一台服务器可以为多台客户端分配IP，如图 14-5所示：

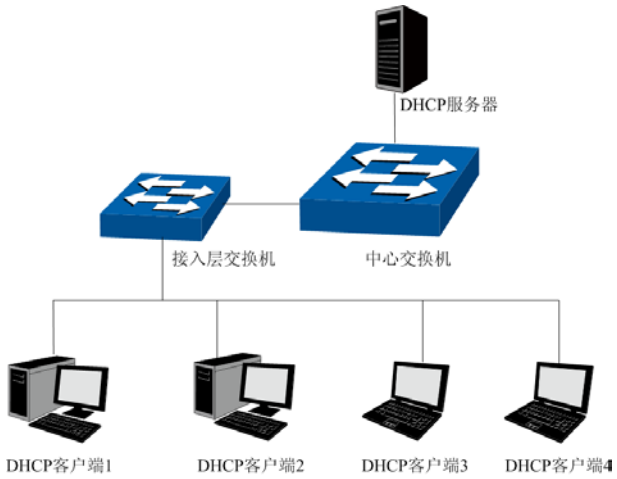


图 14-5 DHCP网络典型应用

针对DHCP客户端的需求不同，DHCP服务器提供三种IP地址分配策略：

1) 手工分配地址：由管理员为少数特定客户端（如WWW服务器等）静态绑定IP地址。通过DHCP将固定IP地址分配给客户端。

2) 自动分配地址：DHCP服务器为客户端分配租期为无限长的IP地址。

3) 动态分配地址：DHCP服务器为客户端分配具有一定有效期限的IP地址，当使用期限到期后，客户端需要重新申请地址。

绝大多数客户端均通过动态分配地址的方式获取IP地址，其获取IP地址的过程如下图所示：

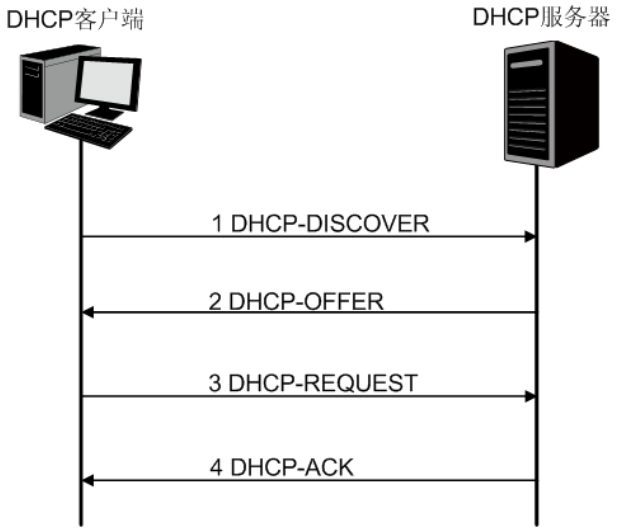


图 14-6 动态获取IP地址的过程

1) 发现阶段，客户端以广播方式发送DHCP-DISCOVER报文寻找DHCP服务器。

2) 提供阶段，DHCP服务器接收到客户端发送的DHCP-DISCOVER报文后，根据IP地址分配的优先次序从地址池中选出一个IP地址，与其它参数一起通过DHCP-OFFER报文发送给客户端（发送方式根据客户端发送的DHCP-DISCOVER报文中的flag字段决定，具体请见DHCP报文格式的介绍）。

3) 选择阶段，如果有多台DHCP服务器向该客户端发来DHCP-OFFER报文，客户端只接受第一个收到的DHCP-OFFER报文，然后以广播方式发送DHCP-REQUEST报文，该报文中包含DHCP服务器在DHCP-OFFER报文中分配的IP地址。

4) 确认阶段，DHCP服务器收到DHCP客户端发来的DHCP-REQUEST报文后，只有DHCP客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回DHCP-ACK报文；否则将返回DHCP-NAK报文，表明地址不能分配给该客户端。

- **Option 82**

DHCP报文格式基于BOOTP的报文格式，共有8种类型的报文，每种报文的格式相同。DHCP和BOOTP消息的不同主要体现在选项（Option）字段，并利用Option字段来实现功能扩展。例如DHCP可以利用Option字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。更多DHCP Option选项的介绍，请参见RFC 2132。

Option 82选项记录了DHCP客户端的位置信息，交换机接收到DHCP客户端发送给DHCP服务器的请求报文后，在该报文中添加Option 82，并转发给DHCP服务器。管理员可以从Option 82中获得DHCP客户端的位置信息，以便定位DHCP客户端，实现对客户端的安全和计费等控制。支持Option 82的服务器还可以根据该选项的信息制订IP地址和其它参数的分配策略，提供更加灵活的地址分配方案。

Option 82最多可以包含255个子选项。若定义了Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路ID子选项）和Remote ID（远程ID子选项）。由于Option 82的内容没有统一规定，不同厂商通常根据需要进行填充。目前本交换机对子选项的填充内容如下，电路ID子选项的填充内容是接收到DHCP客户端请求报文的端口所属VLAN的编号以及端口号，远程ID子选项的填充内容是接收到DHCP客户端请求报文的DHCP侦听设备的MAC地址。

- **DHCP服务欺骗攻击**

在DHCP工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台DHCP服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的DHCP服务器，通常分为两种情况：

1) 用户不小心配置的DHCP服务器，由此引起的网络混乱非常常见。

2) 黑客将正常的DHCP服务器中的IP地址耗尽，然后冒充合法的DHCP服务器，为客户端分配IP地址等配置参数。例如黑客利用冒充的DHCP服务器，为用户分配一个经过修改的DNS服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如图 14-7所示。

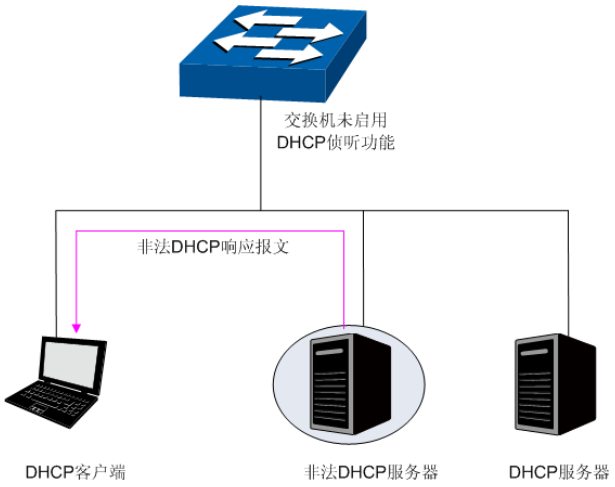


图 14-7 DHCP服务欺骗攻击

DHCP侦听是运行在交换机上的一种DHCP安全特性。通过设置DHCP服务器的连接端口为授信端口，只处理授信端口发来的DHCP响应报文；通过监听DHCP报文，记录用户从DHCP服务器获取局

域网用户的四元信息，进行绑定后与ARP攻击防护、IP源防护等安全功能配合使用；同时也可以过滤不可信任的DHCP信息，防止局域网中发生DHCP服务欺骗攻击，提高网络的安全性。

14.2.1 全局配置

通过DHCP侦听功能，交换机可以侦听用户动态申请IP地址的过程，并记录局域网中计算机的IP地址、MAC地址、VLAN以及连接端口等信息，自动进行四元绑定。交换机还可以利用Option 82字段传递控制信息和网络配置参数，为客户端提供更加丰富的网络配置信息。在全局配置页面中，可以配置DHCP侦听功能全局参数。

进入页面的方法：网络安全>> DHCP侦听>>全局配置

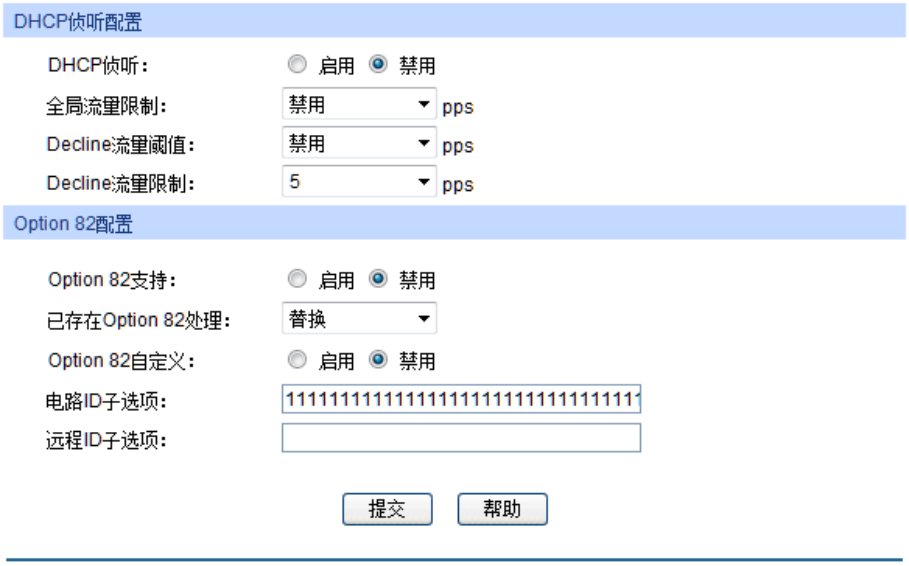


图 14-8 DHCP侦听全局配置

条目介绍：

- **DHCP侦听配置**

  DHCP侦听： 选择是否启用DHCP侦听功能。默认未启用。

  全局流量控制： 填写交换机每秒允许转发的DHCP消息的数目，超出的部分将被丢弃。

  Decline流量阀值： 选择触发特定端口Decline保护所需的Decline报文最小流量。

  Decline流量限制： 如果端口Decline消息流量超出阈值，则将相应端口的端口流量限制设置为该值。

- **Option 82配置**

  Option 82支持： 选择是否启用Option 82字段。默认未启用。

  已存在Option 82处理： 当客户端的DHCP请求报文已经有Option 82字段时，选择对此字段的操作。

  - 保留：保留数据包中的Option字段信息。
  - 替换：替换数据包中的Option字段信息，替换为交换机自定义的系统选项内容。
  - 丢弃：丢弃包含Option 82字段的数据包。

Option 82自定义： 选择交换机是否自定义Option 82选项内容。

电路ID子选项： 输入交换机自定义的Option 82选项中电路ID子选项的内容。

远程ID子选项： 输入交换机自定义的Option 82选项中远程ID子选项的内容。

14.2.2 端口配置

在端口配置页面中，可以配置端口的DHCP侦听功能参数。

进入页面的方法：网络安全>> DHCP侦听>>端口配置

图 14-9 DHCP侦听端口配置参数

条目介绍：

- **端口配置**

UNIT： 根据UNIT ID选择指定交换机进行配置。。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

授信端口： 选择是否配置端口为授信端口，只有授信端口才正常转发来自正常DHCP服务器端的消息，请将连接有DHCP服务器的端口设为授信端口。

MAC验证： 选择是否启用MAC验证功能。DHCP消息中有两个字段存储着客户端的MAC地址，MAC验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

流量控制： 选择是否对DHCP数据包启用流量控制功能，超出流量部分的DHCP数据包将被丢弃。

Decline侦听： 选择是否启用端口的Decline侦听功能。

LAG： 显示端口当前所属的汇聚组。

14.3 ARP 防护

根据 14.1.3 扫描绑定所述的 ARP 地址解析过程可知，利用 ARP 协议，可以实现相同网段内的主机之间正常通信或者通过网关与外网进行通信。但由于 ARP 协议是基于网络中的所有主机或者网关都为可信任的前提制定的，因此在实际复杂的网络中，此过程存在大量的安全隐患，从而导致针对 ARP 协议的欺骗攻击非常常见。网关仿冒、欺骗网关、欺骗终端用户和 ARP 泛洪攻击均是在学校等大型网络中常见的 ARP 攻击，以下简单介绍这几种常见攻击：

- **网关仿冒**

攻击者发送错误的网关 MAC 给受害者，而网络中的受害者收到这些 ARP 响应报文时，自动更新 ARP 表，导致不能正常访问网络。如图 14-10 所示。

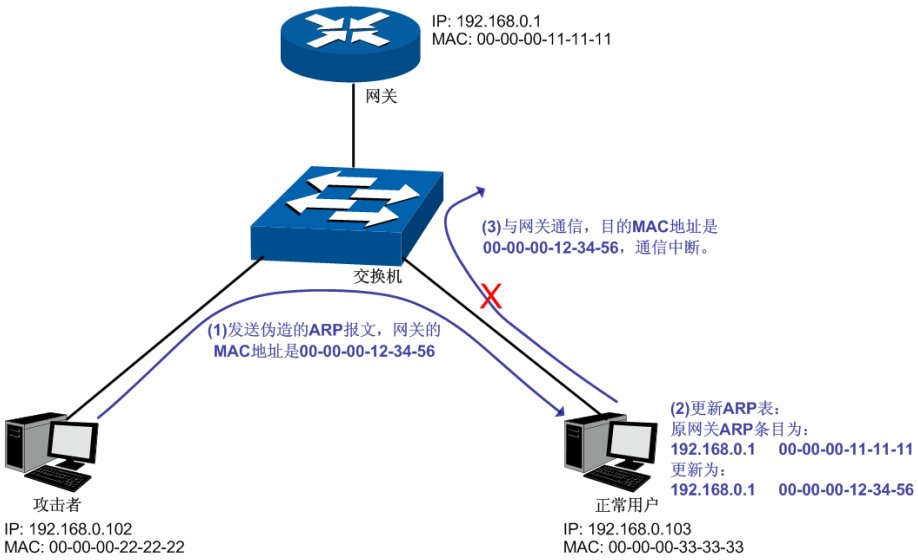


图 14-10 ARP 攻击-网关仿冒示意图

如图，攻击者发送伪造的网关 ARP 报文给局域网中的正常用户，相应的局域网用户收到此报文后更新自己的 ARP 表项。当局域网中正常用户要与网关进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗网关**

攻击者发送错误的终端用户的 IP/MAC 的对应关系给网关，导致网关无法和合法终端用户正常通信。如图 14-11 所示。

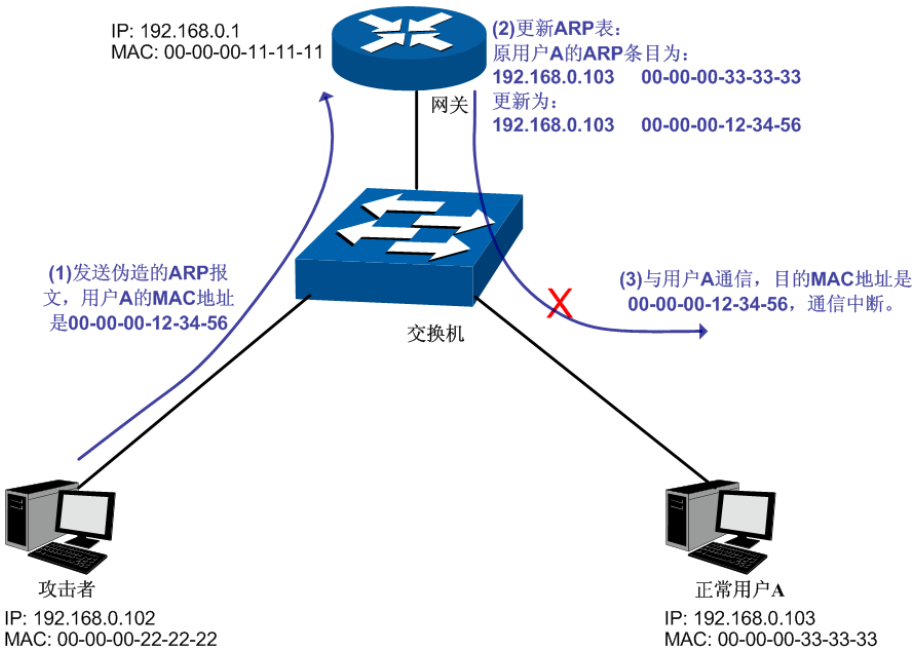


图 14-11 ARP 攻击-欺骗网关示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给网关，网关收到此报文后更新自己的 ARP 表项，当网关与局域网中用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗终端用户**

攻击者发送错误的终端用户/服务器的 IP/MAC 的对应关系给受害的终端用户，导致同网段内两个终端用户之间无法正常通信。如图 14-12 所示。

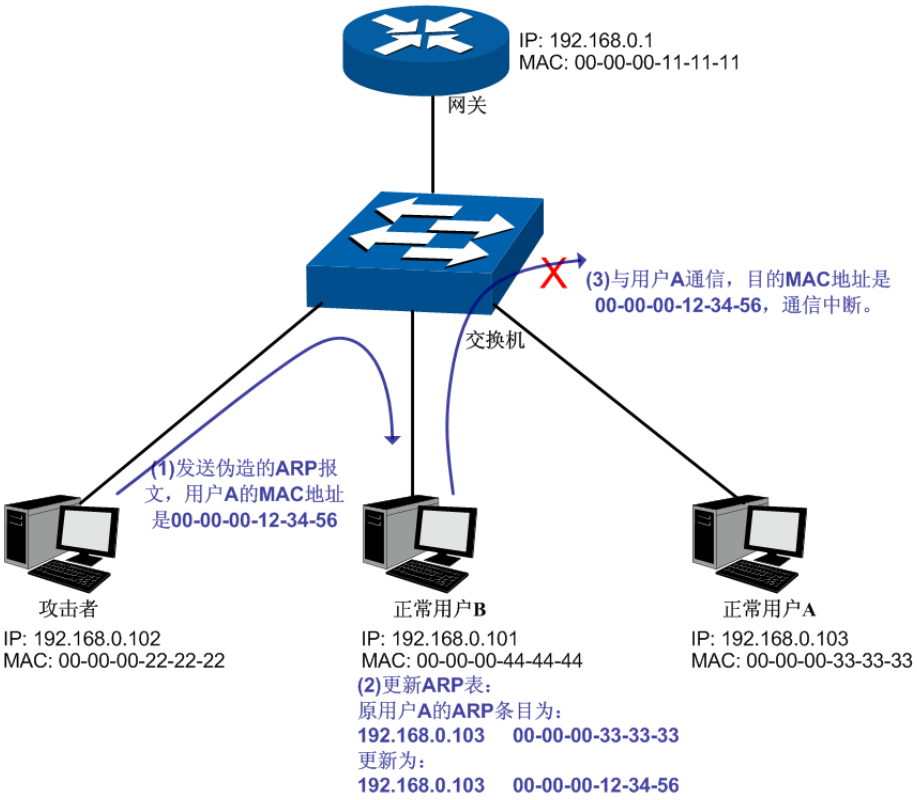


图 14-12 ARP 攻击-欺骗普通用户示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给用户 B，用户 B 收到此报文后更新自己的 ARP 表项，当用户 B 与用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **中间人攻击**

攻击者不断向局域网中计算机发送错误的 ARP 报文，使受害主机一直维护错误的 ARP 表项。当局域网主机互相通信时，将数据包发给攻击者，再由攻击者将数据包进行处理后转发。在这个过程中，攻击者窃听了通信双方的数据，而通信双方对此并不知情。这就是中间人攻击。如图 14-13 所示。

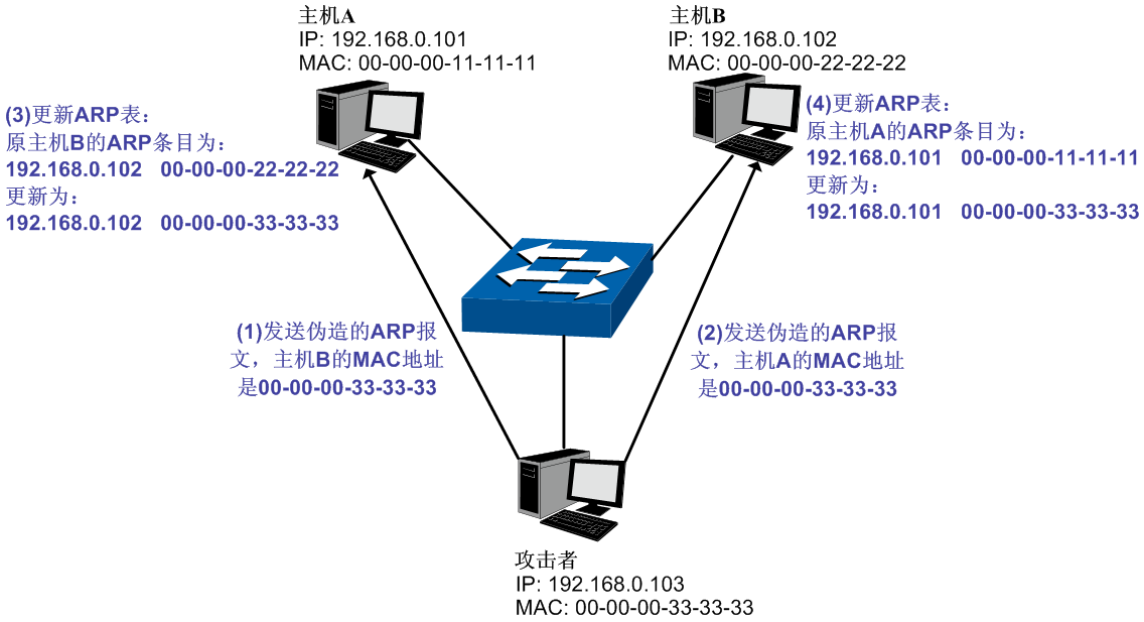


图 14-13 中间人攻击

假设同一个局域网内，有 3 台主机通过交换机相连：

A 主机：IP 地址为 192.168.0.101，MAC 地址为 00-00-00-11-11-11；

B 主机：IP 地址为 192.168.0.102，MAC 地址为 00-00-00-22-22-22；

攻击者：IP 地址为 192.168.0.103，MAC 地址为 00-00-00-33-33-33。

1. 首先，攻击者向主机 A 和主机 B 发送伪造的 ARP 应答报文。
2. A 主机和 B 主机收到此 ARP 应答后，更新各自的 ARP 表。
3. A 主机和 B 主机通信时，将数据包发送给错误的 MAC 地址，即攻击者。
4. 攻击者窃听通信数据后，将数据包重新处理再转发到目标主机，使通信保持畅通。
5. 攻击者连续向 A 主机和 B 主机发送伪造的 ARP 响应报文，使二者始终维护错误的 ARP 表。

在 A 主机和 B 主机看来，彼此发送的数据包都是直接到达对方的，但在攻击者看来，其担当的就是“第三者”的角色。这种嗅探方法，也被称作“中间人”的方法。

- **ARP 泛洪攻击**

攻击者伪造大量不同 ARP 报文在同网段内进行广播，消耗网络带宽资源，造成网络速度急剧降低；同时，网关学习此类 ARP 报文，并更新 ARP 表，导致 ARP 表项被占满，无法学习合法用户的 ARP 表，导致合法用户无法访问外网。

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在 ARP 防护功能中则利用在交换机中绑定的四元信息对 ARP 报文进行检查，过滤非法 ARP 报文。通过上述两步可以很好的对局域网中 ARP 攻击进行防御。

本功能包括**防 ARP 欺骗**、**防 ARP 攻击**和**报文统计**三个功能配置页面。

14.3.1 防 ARP 欺骗

防 ARP 欺骗功能，通过四元绑定表对交换机收到的 ARP 报文进行检查，过滤非法的 ARP 报文，以此防御局域网中的 ARP 攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 欺骗

图 14-14 防 ARP 欺骗

条目介绍：

- **防 ARP 欺骗**

  防 ARP 欺骗： 选择启用并单击<提交>按键即可启用防 ARP 欺骗功能。

- **信任端口**

  信任端口： 勾选无须启用防 ARP 欺骗功能的信任端口。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

注意：

- 防 ARP 欺骗和防 ARP 攻击无法同时启用。

配置步骤：

步骤	操作	说明
1	绑定四元信息条目	必选操作。在**四元绑定**功能中将接入用户的四元信息进行绑定，手动绑定、扫描绑定和 DHCP 侦听方式均可进行绑定。
2	对四元信息条目启用防护	必选操作。在**网络安全>>四元绑定>>绑定列表**页面中对相应的四元条目启用防护。
3	设置信任端口	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中设置信任端口，上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。
4	启用防 ARP 欺骗	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中启用防 ARP 欺骗功能。

14.3.2 防 ARP 攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阀值，在单位时间内不可超过设定值。超过设定值时，交换机将停止处理 ARP 数据包 300 秒，能够有效的避免 ARP 泛洪攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 攻击

图 14-15 防 ARP 攻击

条目介绍：

- **防 ARP 攻击配置**

UNIT：	根据 UNIT ID 选择交换机进行配置。
选择：	勾选端口配置端口防 ARP 攻击功能参数，可多选。
端口：	显示交换机的端口号。
防护功能：	选择是否启用防 ARP 攻击功能。
速率：	填写端口每秒允许接收的 ARP 数据包个数。
当前速率：	显示端口当前收到的 ARP 数据包速率。
状态：	显示端口当前防 ARP 攻击状态。
LAG：	显示端口当前所属的汇聚组。
操作：	点击<恢复>按键使端口恢复正常状态，并重新启用防 ARP 攻击功能。

注意：

- 建议 LAG 端口不要开启防 ARP 攻击功能。
- 防 ARP 欺骗和防 ARP 攻击无法同时启用。

14.3.3 报文统计

通过报文统计功能，可以直观地查看各个端口收到的非法 ARP 数据包个数，并以此定位网络问题，并采取相应的防护措施。

进入页面的方法：网络安全>>ARP 防护>>报文统计

图 14-16 报文统计

条目介绍：

- **自动刷新**

  自动刷新： 设置是否自动刷新端口统计情况。

  刷新周期： 设置自动刷新周期。

- **非法 ARP 报文统计**

  UNIT： 根据 UNIT ID 选择查看指定交换机的统计信息。

  端口： 显示交换机的端口号。

  信任端口： 显示端口是否是 ARP 信任端口。

  非法报文统计： 显示端口收到的非法 ARP 数据包数量。

14.4 IP源防护

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在IP源防护功能中则利用在交换机中绑定的四元信息对IP包进行检查，过滤不符合四元绑定表的IP报文，只处理与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

进入页面的方法：网络安全>>IP源防护

图 14-17 IP源防护

条目介绍：

- **IP源防护配置**

UNIT： 根据UNIT ID选择指定交换机进行配置。

选择： 勾选端口配置端口的IP源防护功能，可多选。

端口： 显示交换机的端口号。

防护类型： 选择端口的防护类型。

- 禁用：禁用端口的IP源防护功能。
- SIP：只处理源IP地址和端口符合四元绑定信息的数据包。
- SIP+MAC：只处理源IP地址、源MAC地址和端口均符合四元绑定信息的数据包。

LAG： 显示端口当前所属的汇聚组。

14.5 DoS防护

DoS（Denial of Service，拒绝服务）攻击是指攻击者利用网络协议实现的缺陷，耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问甚至崩溃。

DoS攻击的具体的影响如下：

1) 耗尽服务器的资源，包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。使服务器疲于响应此类报文，导致网络瘫痪。

2) 由于交换机接收到此类报文需经过CPU处理，因此若请求报文数量过多，会导致交换机CPU利用率持续上升，无法正常工作。

本交换机通过解析IP数据包，分析数据包中的特定字段，并判断是否符合DoS攻击数据包的特征。对于非法的数据包，交换机将直接丢弃；而对于某些正常的数据包，由于流量过大可能导致受害主机瘫痪时，交换机可以对此类数据包进行限速。本交换机能够防护的DoS攻击种类如表 14-1所示。

DoS攻击类型	攻击特征
Land Attack	向目标主机发送一个特别伪造的SYN包，其IP源地址和目的地址都被设置为目标主机的IP地址，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度上降低了系统性能。
Scan SYNFIN	TCP标志位SYN、FIN位被置1的数据包。由于SYN标志用来初始化连接的，FIN标志用来表示发端已完成发送任务请求关闭连接，所以SYN/FIN肯定是非法的数据包，本交换机能够识别此类攻击。
Xmascan	TCP序号置为0，FIN、URG、PSH位置为1的数据包。
NULL Scan	TCP序号置为0，所有控制位置为0的数据包。在正常的TCP连接以及数据传输过程中，不会出现所有控制位置0的情况，此类数据包为非法的数据包。
SYN sPort less 1024	TCP SYN标志位置1，源端口小于1024的数据包。
Blat Attack	数据包的L4源端口等于目的端口且URG置位。此攻击方式类似于Land Attack，被攻击主机因尝试和自己建立连接使系统性能下降。
Ping Flooding	利用Ping广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。
SYN/SYN-ACK Flooding	每当我们进行一次标准的TCP连接，都会有一个三次握手的过程，而TCP-SYN Flood只进行前两个步骤，服务方在一定时间内等待请求方ASK消息。由于一台服务器可用的TCP连接是有限的，如果攻击方发送大量此类连接请求，则服务方TCP连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常的网络服务，从而造成拒绝服务。

表 14-1 本交换机支持的DoS防护种类

在此页面中可以根据实际需要启用合适的DoS防护策略。

进入页面的方法：网络安全>>DoS防护

图 14-18 DoS防护

条目介绍：

- **全局配置**

  DoS攻击防护： 选择是否启用交换机的DoS防护功能。

- **攻击防护列表**

  选择： 勾选启用相应DoS防护。

  防护类型： 显示防护类型。

14.6 802.1X认证

802.1X协议是IEEE802 LAN/WAN委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

本交换机可以作为一个认证系统来对网络中的计算机进行认证。连接在端口上的用户设备如果能通过交换机认证，就可以访问局域网中的资源；如果不能通过交换机认证，则无法访问局域网中的资源。

- **802.1X体系结构**

802.1X的系统是采用典型的Client/Server体系结构，包括三个实体，如图 14-19所示。

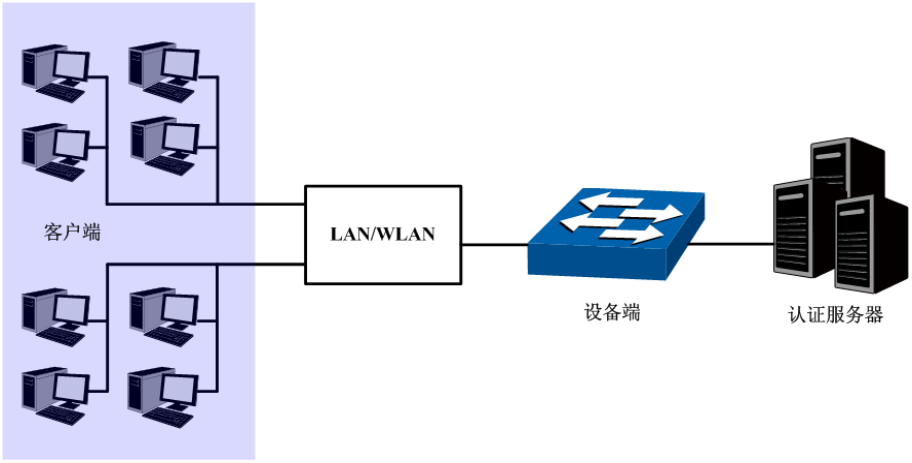


图 14-19 802.1X认证的体系结构

1) 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起802.1X认证，并由设备端对其进行认证。客户端软件必须为支持802.1X认证的用户终端设备。

2) 设备端：通常为支持802.1X协议的网络设备，如本交换机，为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。

3) 认证服务器：为设备端提供认证服务的实体，例如可以使用RADIUS服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

- **802.1X认证工作机制**

IEEE 802.1X认证系统使用EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。

1) 在客户端与设备端之间，EAP协议报文使用EAPOL封装格式，直接承载于LAN环境中。

2) 在设备端与RADIUS服务器之间，可以使用两种方式来交换信息。一种是EAP协议报文使用EAPOR（EAP over RADIUS）封装格式承载于RADIUS协议中；另一种是设备端终结EAP协议报文，采用包含PAP（Password Authentication Protocol，密码验证协议）或CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与RADIUS服务器进行认证。

3) 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端根据RADIUS服务器的指示（Accept或Reject）决定受控端口的授权/非授权状态。

- **802.1X认证过程**

认证过程可以由客户端主动发起，也可以由设备端发起。一方面当设备端探测到有未经过认证的用户使用网络时，就会主动向客户端发送EAP-Request/Identity报文，发起认证；另一方面客户端可以通过客户端软件向设备端发送EAPOL-Start报文，发起认证。

802.1X系统支持EAP中继方式和EAP终结方式与远端RADIUS服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP中继方式

EAP中继方式是IEEE 802.1X标准规定的，将EAP（扩展认证协议）承载在其它高层协议中，如EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP中继方式需要RADIUS服务器支持EAP属性：EAP-Message和Message-Authenticator。本交换机支持的EAP中继方式是EAP-MD5，EAP-MD5认证过程如图 14-20所示。

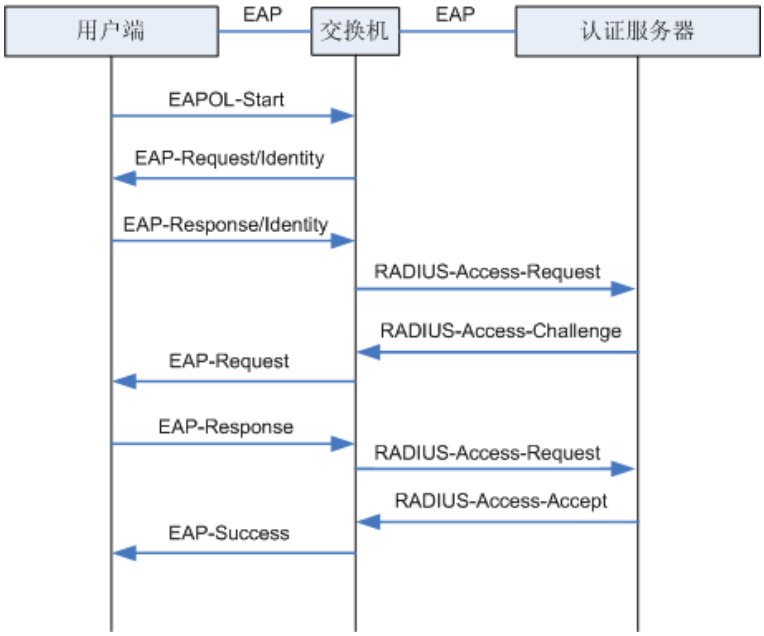


图 14-20 EAP-MD5认证过程

1) 当用户有访问网络需求时打开802.1X客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity报文）要求用户的客户端程序发送输入的用户名。

3) 客户端程序响应设备端发出的请求， 将用户名信息通过数据帧（EAP-Response/Identity报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request报文）送给认证服务器进行处理。

4) RADIUS服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过RADIUS Access-Challenge报文发送给设备端，由设备端转发给客户端程序。

5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的，生成EAP-Response/MD5 Challenge报文），并通过设备端传给认证服务器。

6) RADIUS服务器将收到的已加密的密码信息（RADIUS Access-Request报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept报文和EAP-Success报文）。

7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8) 客户端也可以发送EAPOL-Logoff报文给设备端，主动要求下线，设备端把端口状态从授权状态改变成未授权状态。

2. EAP终结方式

EAP终结方式将EAP报文在设备端终结并映射到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。设备端与RADIUS服务器之间可以采用PAP或者CHAP认证方法。本交换机支持的EAP终结方式是PAP，PAP认证过程如图 14-21所示。

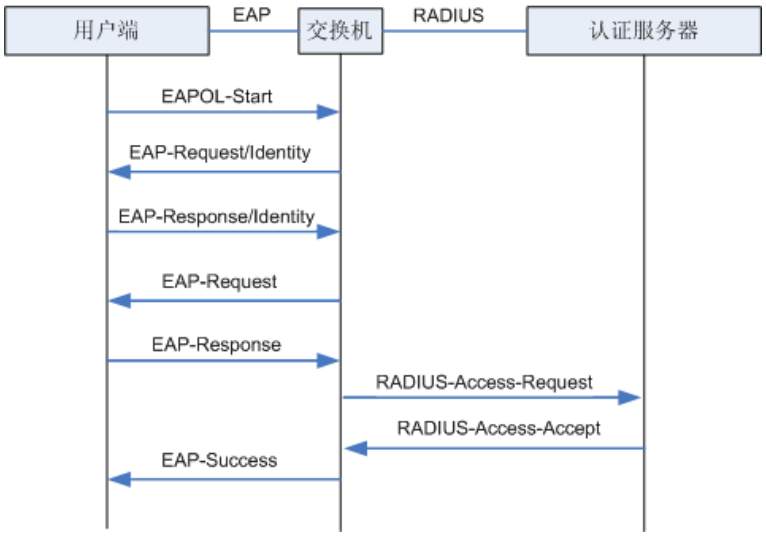


图 14-21 PAP认证过程

在PAP模式中，交换机对用户口令信息进行加密，然后把用户名、随机加密字和客户端加密后的口令信息一起转发给认证服务器进行相关的认证处理；而在EAP-MD5模式中，随机加密字由认证服务器产生，交换机只负责把认证信息报文封装后转发。

- **802.1X定时器**

802.1X认证过程中会启动多个定时器以控制接入用户、设备以及RADIUS服务器之间进行合理、有序的交互。本交换机中的802.1X定时器主要有以下三种：

1) **客户端认证超时定时器**：当交换机向客户端发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到客户端的响应，交换机将重发该报文。

2) **认证服务器超时定时器**：当交换机向认证服务器发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到认证服务器的响应，交换机将重发认证请求报文。

3) **静默定时器**：对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设置），在静默期间，交换机不再处理该用户的认证请求。

- **Guest VLAN**

Guest VLAN功能用来允许未通过认证的用户访问某些特定资源。用户认证端口在通过802.1X认证之前属于Guest VLAN，用户访问该VLAN内的资源不需要认证，但此时不能够访问其它网络资源；认证成功后，端口离开Guest VLAN，用户可以访问其它的网络资源。

用户可以在Guest VLAN中获取802.1X客户端软件、升级客户端或执行其它一些用户升级程序。如果因为没有专用的认证客户端或者客户端版本过低等原因，导致一定的时间内端口上无客户端认证成功，本交换机会把该端口加入到Guest VLAN。

开启802.1X特性并正确配置Guest VLAN后，当交换机向客户端发送EAP-Request/Identity报文而没有收到客户端的回应时，该端口将按照各自的链路类型被加入到Guest VLAN内。此时如果Guest VLAN中有用户发起认证且认证失败，相应连接端口仍会留在Guest VLAN内；如果认证成功，端口离开Guest VLAN，加入配置的VLAN中。用户下线后，端口将返回Guest VLAN中。

本交换机802.1X认证功能包括**全局配置**、**端口配置**和**RADIUS配置**三个配置页面。

14.6.1 全局配置

在全局配置功能页面，可以开启全局802.1X认证功能，选择本交换机提供的认证方法，并设置Guest VLAN以及各种定时器来协调整个系统的802.1X认证过程。

进入页面的方法：网络安全>>802.1X认证>>全局配置

图 14-22 全局配置

条目介绍：

- **全局配置**

802.1X功能： 选择是否启用802.1X认证功能。

认证方法： 选择802.1X认证方法。

- EAP-MD5：交换机与认证服务器之间运行EAP协议，EAP帧中封装认证数据，将该协议承载在其它高层次协议中(如RADIUS)，以便穿越复杂的网络到达认证服务器。
- PAP：用户端与交换机之间运行EAP协议，交换机将EAP消息转换为其它认证协议(如RADIUS)，传递用户认证信息给认证服务器系统。

Guest VLAN： 选择是否启用Guest VLAN功能。

Guest VLAN ID： 填写启用Guest VLAN的VLAN ID。Guest VLAN中的用户可以访问指定的网络资源。

➢ **认证参数配置**

静默： 选择是否启用静默计时器。

静默时长： 填写静默时长。用户认证失败后，在静默时间内不再处理同一用户的802.1X认证请求。

重复发送次数： 填写认证报文的最大重传次数。

客户端响应超时： 填写交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。

服务器响应超时： 填写交换机等待服务器响应的最大等待时间。若交换机在设定时间内没有收到服务器的回复，则重发报文。

14.6.2 端口配置

在端口配置功能页面，可以根据实际的网络情况设置端口的802.1X功能特性。

进入页面的方法：网络安全>>802.1X认证>>端口配置

图 14-23 端口配置

条目介绍：

➢ **端口配置**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选端口，配置端口的802.1X认证状态，可多选。

端口： 显示交换机端口号。

状态： 选择该端口是否启用802.1X认证。

Guest VLAN： 选择该端口是否启用Guest VLAN。

控制模式： 选择该端口的控制模式。

- 自动：端口需要进行认证。
- 强制已认证：端口不需要认证即可访问网络。
- 强制不认证：端口永远无法通过认证。

控制类型： 选择该端口的控制类型。

- 基于MAC：该端口连接的所有计算机都需要认证。
- 基于Port：该端口连接的某个用户通过认证后，其它用户均无须认证即可访问网络。

授权状态： 显示此端口的授权状态。

LAG： 显示端口当前所属的汇聚组。

14.6.3 RADIUS配置

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）认证服务器为交换机提供认证服务，其存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户进行认证、授权和计费。RADIUS配置功能页面用来设置网络中认证服务器的参数，保证认证过程通畅有序的进行。

进入页面的方法：网络安全>>802.1X认证>>RADIUS配置

图 14-24 RADIUS配置

条目介绍：

- **认证服务器配置**

服务器IP： 填写认证服务器的IP地址。

备份服务器IP： 填写备份认证服务器的IP地址。

认证端口： 填写认证服务器提供认证服务的协议端口。

授权共享密钥： 填写交换机与服务器共享的密钥。

- **计费服务器配置**

计费功能： 选择是否启用计费功能。

服务器IP： 填写计费服务器的IP地址。

备份服务器IP： 填写备份计费服务器的IP地址。

计费端口： 填写计费服务器提供计费服务的协议端口。

授权共享密钥： 填写交换机与服务器共享的密钥。

注意：

- 只有同时开启全局和端口的802.1X特性后，才能使802.1X认证功能生效。
- LAG端口不能启用802.1X功能。如果端口启动了802.1X，则不能配置该端口加入聚合组。
- 认证服务器连接的端口请勿开启802.1X特性，且服务器配置参数必须与认证服务器软件的参数一致。

配置步骤：

步骤	操作	说明
1	搭建认证服务器	必选操作。搭建完成后，请在服务器中记录局域网接入用户的信息并设置相应的用户名和密码以备认证。
2	安装客户端软件	必选操作。请在接入计算机中安装光盘中的802.1X客户端软件，安装过程见附录A 802.1X客户端软件使用说明。
3	设置802.1X全局参数	必选操作。默认情况下，交换机802.1X全局功能未开启，请在**网络安全>>802.1X认证>>全局配置**页面中设置全局参数。
4	设置认证服务器参数	必选操作。请自行搭建认证服务器，并在**网络安全>>802.1X认证>>RADIUS配置**页面中设置服务器参数。
5	设置各端口802.1X功能参数	必选操作。请在**网络安全>>802.1X认证>>端口配置**页面中根据实际网络情况设置交换机各端口的802.1X功能参数。

回目录

第15章 SNMP

➢ SNMP概述

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前UDP/IP网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。SNMP结构简单，使用方便，并且能够屏蔽不同设备的物理差异，实现对不同设备的自动化管理，所以得到了广泛的支持和应用，目前大多数网络管理系统和平台都是基于SNMP的。

SNMP的最大优势就是设计简单，他既不需要复杂的实现过程，也不会占用太多的网络资源，便于使用。SNMP的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP可实现统计、配置和测试等功能；当网络出故障时，可实现各种错误检测和恢复功能。

➢ SNMP的管理框架

SNMP包括三个网络元素：SNMP管理者(SNMP Manager)，SNMP代理(SNMP Agent)，MIB库（Management Information Base，管理信息库）。

SNMP管理者：运行在SNMP客户端程序的工作站，提供了非常友好的人机交互页面，方便网络管理员完成绝大多数的网络设备管理工作。

SNMP代理：驻留在被管理设备上的一个进程，负责接受、处理来自SNMP管理者的请求报文。在一些紧急情况下，SNMP代理也会通知SNMP管理者事件的变化。

MIB库：被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个SNMP代理都有自己的MIB。SNMP管理者根据权限可以对MIB中的对象进行读/写操作。

SNMP管理者是SNMP网络的管理者，SNMP代理是SNMP网络的被管理者，他们之间通过SNMP协议来交互管理信息。SNMP管理者、SNMP代理、MIB库三者的关系如图 15-1所示。

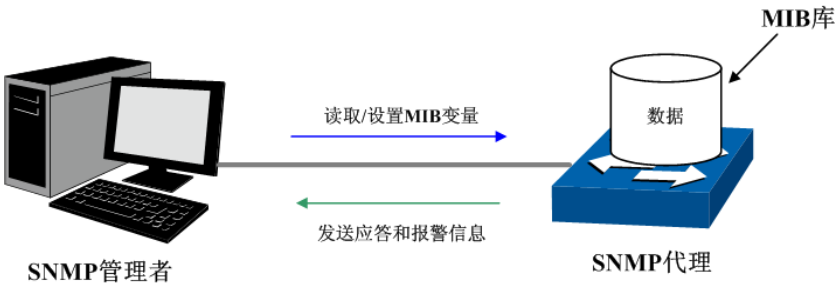


图 15-1 SNMP网元关系图

➢ SNMP的协议版本

本交换机提供了SNMPv3的管理功能，同时兼容SNMPv1和SNMPv2c，SNMP管理者和SNMP代理的SNMP版本需要一致，它们之间才能相互通信，可以根据自己的应用需求，选择不同安全级别的管理模式。

SNMPv1：采用团体名（Community Name）认证。团体名用来定义SNMP管理者和SNMP代理的关系。如果SNMP报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制SNMP管理者对SNMP代理的访问。

SNMPv2c：也采用团体名认证。它在兼容SNMPv1的同时又扩充了SNMPv1的功能。

SNMPv3：SNMPv3在前两个版本v1、v2c的基础上大大加强了安全性和用户可控制性，采用了VACM（View-based Access Control Model，基于视图的访问控制模型）及USM（User-Based Security

Model，基于用户的安全模型）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对SNMP管理者和SNMP代理之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为SNMP管理者和SNMP代理之间的通信提供更高的安全性。

➢ **MIB库简介**

MIB是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，被管理对象可以用一串数字唯一确定，这串数字是被管理对象的OID（Object Identifier，对象标识符）。MIB的结构如图 15-2所示。图中，B的OID为{1.2.1.1}，A的OID为{1.2.1.1.5}。

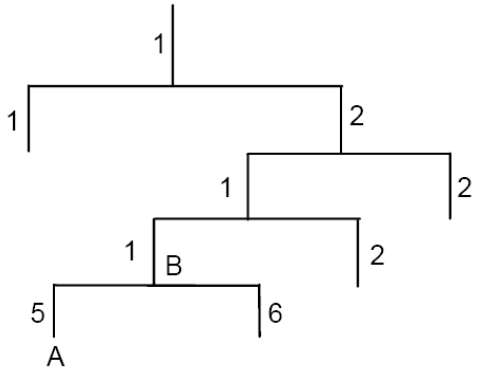


图 15-2 MIB树结构

➢ **SNMP配置概要**

- 创建视图

MIB视图是全部MIB管理对象的一个子集。管理对象以OID（Object Identifier，对象标识符）来表示，通过配置管理对象的视图类型（包括/排除），来达到控制该管理对象能否被管理的目的。各管理对象的OID可以在SNMP管理软件上找到。

- 创建SNMP组

创建完视图之后，需要创建SNMP组，只有“组名”、“安全模式”、“安全级别”三项均相同的组，才被认为是同一个组。同时可以为各个SNMP组添加只读/只写/通知视图，从而满足了处于不同组内的用户对交换机功能的访问权限不同的需求。

- 创建用户

用户创建于SNMP组中，SNMP管理端使用此处创建的用户及其认证/加密密码来登录SNMP代理端。

SNMP模块主要用于配置交换机的SNMP功能，包括**SNMP配置**、**通知管理**和**RMON**三个部分。

15.1 SNMP配置

在本功能处可以配置SNMP的各项基本功能，包括**全局配置**、**视图管理**、**组管理**、**用户管理**和**团体管理**五个配置页面。

15.1.1 全局配置

配置交换机的SNMP功能，首先需要在本页配置交换机SNMP的全局功能。

进入页面的方法：SNMP>>SNMP配置>>全局配置

图 15-3 全局配置

条目介绍：

- **全局配置**

  SNMP功能： 选择是否启用交换机的SNMP功能。

- **本地引擎配置**

  本地引擎ID： 填写本地SNMP实体的引擎ID。本地用户建立在本地引擎之下。

- **远程引擎配置**

  远程引擎ID： 填写SNMP管理端的引擎ID。远程用户建立在远程引擎之下。

注意：

- 引擎ID的字符个数必须为偶数。

15.1.2 视图管理

在SNMP报文中使用管理变量（OID）来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。本页用来配置SNMP的视图。

进入页面的方法：SNMP>>SNMP配置>>视图管理

图 15-4 视图管理

条目介绍：

- **新建视图**

  视图名称： 填写视图条目的名称。一个视图可以有多个同名的视图条目。

  MIB子树OID： 填写该视图条目的管理变量（OID）。

  视图类型： 选择OID的类型。

  - 包括：该OID可以被管理软件管理。
  - 排除：该OID不能被管理软件管理。

- **视图列表**

  选择： 勾选条目进行删除。同一视图下的所有视图条目会被同时选择。

  视图名称： 显示视图名称。

  类型： 显示对应OID的类型。

  MIB子树OID： 显示对应视图下的管理变量（OID）。

15.1.3 组管理

本页用来配置SNMP的组，组内的用户通过只读、只写、通知视图来达到访问控制的目的。

进入页面的方法：**SNMP>>SNMP配置>>组管理**

图 15-5 组管理

条目介绍：

- **组配置**

组名： 填写组名。与“安全模式”和“安全级别”三项共同组成该组的标识，三项均相同才被认为是同一组。

安全模式： 选择组的安全模式。

- v1：SNMP v1，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v2c：SNMP v2c，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v3：SNMP v3，采用USM认证。

安全级别： 选择SNMP v3的组的安全级别。

只读视图： 选择只读视图，对所选的视图只能被查看不能被编辑。

只写视图： 选择只写视图，对所选的视图只能被编辑不能被查看。若您想要进行读写操作，则需要同时在“只读视图”中添加。

通知视图： 选择通知视图，管理软件可以接收到所选视图发送的异常警报信息。

- **组列表**

选择： 勾选条目进行删除，可多选。

组名： 显示SNMP组的组名。

安全模式： 显示组的安全模式。

安全级别： 显示组的安全级别。

只读视图： 显示组中具有只读权限的视图名称。

只写视图： 显示组中具有只写权限的视图名称。

通知视图： 显示组中具有通知权限的视图名称。

操作： 点击对应条目的<编辑>按键，可以修改该条目的视图。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 一个组必须具备一个只读视图，默认只读视图为viewDefault。

15.1.4 用户管理

SNMP管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。本页用来配置SNMP的用户。

进入页面的方法：SNMP>>SNMP配置>>用户管理

图 15-6 用户管理

条目介绍：

- **用户配置**

用户名： 填写用户名。

用户类型： 选择用户类型。

- 本地用户：建立在本地引擎下的用户。
- 远程用户：建立在远程引擎下的用户。

组名： 选择组名。通过“组名”、“安全模式”、“安全级别”来确定用户所属的组。

安全模式： 选择安全模式。

安全级别： 选择安全级别。

认证模式： 选择SNMP v3用户的认证模式。

- 无：不认证。
- MD5：信息摘要算法。
- SHA：安全散列算法，比MD5的安全性更高。

认证密码： 输入认证密码。

加密模式： 选择SNMP v3用户的加密模式。

- 无：不加密。
- DES：数据加密标准。

加密密码： 输入加密密码。

➢ **用户列表**

选择： 勾选条目进行删除，可多选。

用户名： 显示用户名。

用户类型： 显示用户类型。

组名： 显示组名。

安全模式： 显示安全模式。

安全级别： 显示安全级别。

认证模式： 显示认证模式。

加密模式： 显示加密模式。

操作： 点击对应条目的<编辑>按键，可以修改该用户所属的组。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

15.1.5 团体管理

SNMP v1和SNMP v2c采用团体名（Community Name）认证，团体名起到了类似于密码的作用。若您使用的是SNMP v1和SNMP v2c，配置完视图之后，可以直接在本页配置SNMP的团体。

进入页面的方法：SNMP>>SNMP配置>>团体管理

图 15-7 团体管理

条目介绍：

- **团体配置**

  团体名： 填写团体名。

  权限： 选择该团体对视图的访问权限。
  - 只读：团体对相应视图具有只读权限。
  - 读写：团体对相应视图具有读写权限。

  MIB视图： 选择团体可访问的视图。

- **团体列表**

  选择： 勾选条目进行删除，可多选。

  团体名： 显示团体名。

  权限： 显示团体对视图的访问权限。

  MIB视图： 显示团体可访问的视图。

  操作： 点击对应条目的<编辑>按键，可以修改该团体的访问视图及访问权限。修改完毕后点击<修改>按键，修改内容生效。

注意：
- 团体的默认MIB视图为viewDefault。

SNMP功能配置步骤：

- 若您使用SNMPv3版本

步骤	操作	说明
1	启用SNMP全局功能	必选操作。在**SNMP>>SNMP配置>>全局配置**页面，启用交换机的SNMP功能。
2	创建视图	可选操作。在**SNMP>>SNMP配置>>视图管理**页面，创建管理对象的视图。默认视图名为viewDefault，OID为1。
3	创建SNMP组	必选操作。在**SNMP>>SNMP配置>>组管理**页面，创建SNMPv3类型的组，并为组添加不同访问权限的视图。
4	创建SNMP组内的用户	必选操作。在**SNMP>>SNMP配置>>用户管理**页面，创建SNMPv3组内的用户，并配置用户的认证/加密模式及密码。

- 若您使用SNMPv1版本或SNMPv2c版本

步骤	操作	说明
1	启用SNMP全局功能。	必选操作。在**SNMP>>SNMP配置>>全局配置**页面，启用交换机的SNMP功能。
2	创建视图	可选操作。在**SNMP>>SNMP配置>>视图管理**页面，创建管理对象的视图。默认视图名为viewDefault，OID为1。

步骤	操作			说明
3	配置访问权限	直接设置	创建团体	二者必选其一。 • 直接设置是在**SNMP>>SNMP配置>>团体管理**页面，以SNMPv1和v2c版本的团体名进行设置。 • 间接设置采用与SNMPv3版本一致的命令形式，添加用户到v1/v2c类型的组，即相当于SNMPv1和SNMPv2c版本的团体名。在SNMP管理软件上用来登录交换机的团体名需要跟这里配置的用户名一致，该组下创建的v1/v2c用户（团体）的读、写视图与该组的读写视图对应。
		间接设置	创建SNMP组	
			创建SNMP组内的用户	

15.2 通知管理

通知管理功能是交换机主动向管理软件报告某些视图的重要事件（如设备重启等），便于管理员通过管理软件对交换机一些特定事件进行及时监控和处理。

通知报文分为以下两种：

Trap：发送Trap报文通知SNMP管理者。

Inform：发送Inform报文通知SNMP管理者，并且要求SNMP管理者返回信息。交换机发送Inform报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送该Inform报文。Inform具有更高的可靠性，在SNMP v2c和SNMP v3中均可以使用。

本页用来配置SNMP的通知管理功能。

进入页面的方法：SNMP>>通知管理>>通知管理

图 15-8 通知管理

条目介绍：

- **新建条目**

目的IP地址： 填写管理主机的IP地址。

UDP端口： 填写管理主机上启用供通知过程使用的UDP端口，与IP地址共同作用。默认为162。

团体名/用户名： 配置管理软件的团体名/用户名。

安全模式： 选择用户的安全模式。

安全级别： 配置SNMP v3的用户的安全级别。

通知类型： 选择使用的通知报文的类型。

- Trap：以Trap方式发送通知。
- Inform：以Inform方式发送通知，Inform具有更高的可靠性。

重传： 填写Inform报文的重传次数。交换机发送Inform报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送Inform报文。默认为3。

超时： 填写交换机等待Inform回应报文的时间。超过该时间后，将重新发送Inform报文。默认为100秒。

➢ **目的主机列表**

选择： 勾选条目进行删除，可多选。

目的IP地址： 显示管理主机的IP地址。

UDP端口： 显示管理主机上启用供通知过程使用的UDP端口。

团体名/用户名： 显示管理软件的团体名/用户名。

安全模型： 显示用户的安全模式。

安全级别： 显示SNMP v3的用户的安全级别。

通知类型： 显示使用的通知报文的类型。

超时： 显示Inform报文的重传次数。

重传： 显示收到Inform报文回应报文的超时时间。

操作： 点击对应条目的<编辑>按键，可以修改该通知条目的参数。修改完毕后点击<修改>按键，修改内容生效。

15.3 RMON

RMON（Remote Monitoring，远程网络监视）完全基于SNMP体系结构，是IETF（Internet Engineering Task Force，因特网工程任务组）提出的标准监控规范，他使SNMP更为有效、更为积极主动地监控远程设备。利用RMON功能，网管可以快速跟踪网络、网段或设备出现的故障，积极采取防范措施，防止网络资源的失效，同时RMON MIB也可以记录网络性能和故障的数据，您可以在任何时候访问历史数据从而进行有效的故障诊断。RMON减少了SNMP管理者同代理间的通信流量，使得网管可以简单而有效地管理大型网络。

➢ **RMON的工作原理**

RMON代理在RMON MIB中存储网络信息，交换机置入RMON代理后，具有了RMON探测的功能。管理者使用SNMP的基本命令与RMON代理交互数据信息，收集网络管理信息。但是由于设备资源的限制，管理者无法获取RMON MIB的全部数据，一般只可以收集到四个组的信息，这四个组是：历史组、事件组、统计组和警报组。

➢ **RMON组**

本交换机支持RMON规范（RFC1757）中定义的历史组、事件组、统计组和警报组。

RMON组	功能	元素
历史组	周期性地收集网络统计信息，存储起来以便日后提取，从而有效的监测网络。	采样端口、采用间隔、创建者。
事件组	定义事件序号及事件的处理方式。此处定义的事件主要用在警报组中警报触发产生的事件。	事件描述、事件类型、创建者、用户名。
统计组	监测报警变量在指定端口的统计值。	丢弃数据包、丢弃字节、数据包发送、广播数据包、组播数据包、CRC错误帧、过小（或超大）的数据报文、冲突帧以及各种长度的数据包，包括64、65~127、128~255、256~511、512~1023以及1024~10240字节。
警报组	定期对指定的警报变量进行监测，一旦计数器超过阈值则触发警报。	警报变量、样例类型、时间间隔、阈值上限、阈值下限、警报触发方式。

在本功能处可以配置RMON的各个组，包括**历史组**、**事件组**和**警报组**四个配置页面。

15.3.1 统计组

本页用来配置RMON的统计组。统计组统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控、统计。该组包含一个以太网统计表，统计的内容包括丢弃的数据包、广播数据包、CRC错误、大小块、冲突等。现最多只支持1000条。

进入页面的方法：SNMP>>RMON>>统计组

图 15-9 统计组配置

条目介绍：

➢ **统计组配置**

ID号： 填写统计条目的ID号，大小范围为1~65535。

端口： 填写或者选择被统计的以太网端口。

创建者： 填写创建这一条目的用户名。

状态： 选择条目的状态。

- 生效：条目存在且生效。
- 未生效：条目存在，但暂时未生效。

➢ **统计条目列表**

在列表区查看已存在的统计组条目的配置信息。

15.3.2 历史组

本页用来配置RMON的历史组。

进入页面的方法：SNMP>>RMON>>历史组

历史采样控制

选择	序号	采样端口	采样间隔（秒）	最大采样数目	创建者	状态
	1	1/0/1	1800	50	monitor	禁用
	2	1/0/1	1800	50	monitor	禁用
	3	1/0/1	1800	50	monitor	禁用
	4	1/0/1	1800	50	monitor	禁用
	5	1/0/1	1800	50	monitor	禁用
	6	1/0/1	1800	50	monitor	禁用
	7	1/0/1	1800	50	monitor	禁用
	8	1/0/1	1800	50	monitor	禁用
	9	1/0/1	1800	50	monitor	禁用
	10	1/0/1	1800	50	monitor	禁用
	11	1/0/1	1800	50	monitor	禁用
	12	1/0/1	1800	50	monitor	禁用

全选 提交 帮助

图 15-10 历史组

条目介绍：

➢ **历史采样控制**

选择： 勾选条目配置采样属性。

序号： 显示采样条目的序号。

采样端口： 选择进行采样的端口。

采样间隔： 填写端口采样的时间间隔。默认为1800秒。

最大采样数目： 显示当前历史控制表项所能够保存的采样数据条目的最大数目，目前最多仅支持130条。范围为1~65535，默认值为50。

创建者： 填写创建该采样条目的实体。

状态： 选择是否启用所选采样条目。

15.3.3 事件组

本页用来配置RMON的事件组。

进入页面的方法：**SNMP>>RMON>>事件组**

图 15-11 事件配置

条目介绍：

- **事件配置**

选择： 勾选条目配置事件属性。

序号： 显示事件条目的序号。

用户名： 填写事件所属的用户。当对应事件需要发送通知时，将会根据此用户名进行发送。

描述： 填写该事件的描述信息。

类型： 选择事件的类型。

- 无：不做任何操作。
- 日志：将事件记录在交换机中，通过SNMP管理软件读取。
- 通知：向管理主机发送报警消息。
- 日志&通知：将事件记录在交换机中并向管理主机发送报警消息。

创建者： 填写创建该事件条目的实体。

状态： 选择是否启用所选事件条目。

15.3.4 警报组

本页用来配置RMON的警报组。

进入页面的方法：SNMP>>RMON>>警报组

图 15-12 警报组配置

条目介绍：

- **警报配置**

选择： 勾选条目配置警报属性。

序号： 显示警报条目的序号。

计数器： 选择警报变量。

样例类型： 为警报变量选择取样的方法，再将取样的值与阈值进行比较。

- 绝对值：在一个取样周期结束时将取样结果与阈值进行比较。
- 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。

上升阈值： 填写触发警报的上升阈值。默认为100。

上升事件： 选择触发上升阈值警报的事件的序号。

下降阈值： 填写触发警报的下降阈值。默认为100。

下降事件： 选择触发下降阈值警报的事件的序号。

启动警报： 选择警报触发的方式。

- 上升：只在触发上升阈值后触发警报。
- 下降：只在触发下降阈值后触发警报。
- 全部：触发上升和下降阈值均触发警报。

时间间隔： 填写警报的时间间隔。默认为1800秒。

创建者： 填写创建该警报条目的实体。

状态： 选择是否启用所选警报条目。

注意：

- 当警报变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生警报事件。即上升警报和下降警报是交替产生的，出现了一次上升警报，则下一次必为下降警报。

回目录

第16章 LLDP

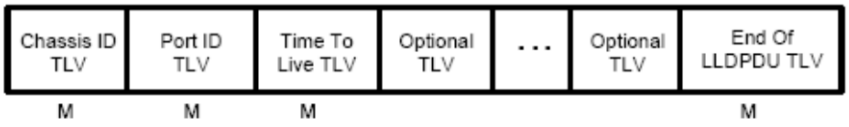
链路层发现协议LLDP（Link Layer Discovery Protocol）是一个二层协议，在符合IEEE802标准的局域网络中，允许网络设备周期性地向邻居设备通告自己的设备信息。LLDP根据IEEE802.1AB标准把设备的标识、性能和配置等信息组织成不同的TLV（Type/Length/Value，类型/长度/值），并封装在LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给邻居设备，邻居设备收到这些信息后将其以标准的MIB（Management Information Base，管理信息库）形式保存起来。网络管理系统可以通过管理协议SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息，以查询及判断链路的通信状况。

为了描述网络的物理拓扑和拓扑中的相关系统，IETF（Internet Engineering Task Force, 互联网工程任务组）组织提出了标准MIB，一些公司也提出了私有MIB。但是，IEEE 802局域网站点并没有统一的标准来传输MIB信息。LLDP解决了这一问题。LLDP协议允许不同厂商的网络设备协同工作，运行LLDP协议的设备能够自动检测并学习邻居设备的信息。LLDP还可以使运行不同网络层协议的系统互相学习对方的设备信息。

SNMP应用可以利用LLDP获取的信息，进行网络故障排除，从而提高网络的稳定性，维持正确的网络拓扑。

➢ LLDPDU

每一个LLDPDU携带四个必须的TLV以及一个或者多个可选的TLV。如下图所示，Chassis ID TLV, Port ID TLV, TTL TLV 和 End TLV是每个LLDPDU所必须携带的四个TLV。可选的TLV是由网络管理系统决定的，它们提供了关于本地LLDP设备的详细信息。



M - mandatory TLV - required for all LLDPDUs

LLDPDU的最大长度由特定的传输速率和协议所允许的最大报文长度决定。就IEEE 802.3 MAC协议来说，LLDPDU的最大长度是不带TAG的基本MAC帧的最大长度，即1500字节。

➢ LLDP工作机制

1) LLDP的工作模式

每个端口都可以分别配置LLDPDU的接收和发送功能，这样端口可以配置四种工作模式：

- 发送接收：既发送也接收LLDPDU。
- 只接收：只对接收到的LLDPDU进行处理，而不向外发送LLDPDU。
- 只发送：只向外发送LLDPDU，而不对接收到的LLDPDU进行处理。
- 禁用：既不向外发送LLDPDU，也不对接收到的LLDPDU进行处理。

2) LLDPDU的传输机制

- 当端口工作在发送接收模式或者只发送模式时，设备会周期性地向邻居设备发送LLDPDU以通告自己的信息。

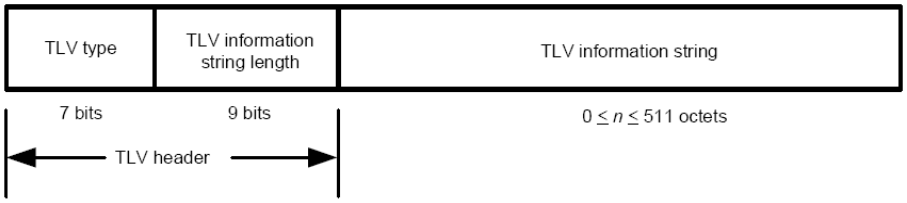
- 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避免设备连续地发送LLDPDU而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保LLDPDU的发送有一个固定的最小时间差。
- 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为1s，快速发出一些LLDPDU之后，设备恢复正常的发送周期。

3) LLDPDU的接收机制

当端口工作在发送接收模式或只接收模式时，设备会对收到的LLDP报文及其携带的TLV进行有效性检查，通过检查后再将邻居信息保存到本地，并根据TTL（Time To Live，生存时间）TLV中TTL的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

➢ TLV

TLV是LLDPDU的基本组成单位，是Type/Length/Value的简称，即类型/长度/值。基本TLV的格式如下图所示：



每个TLV的类型都是不一样的，根据TLV的类型可以判断TLV中的信息类型。

下表是目前定义的各种TLV的详细信息。

TLV 类型	TLV 名称	说明	是否必须携带
0	End of LLDPDU	标识LLDPDU结束，任何在End Of LLDPDU TLV之后的信息将被丢弃	是
1	Chassis ID	标识连接设备的Chassis ID	是
2	端口ID	标识发送端口的ID信息	是
3	Time To Live	本地设备信息在邻居设备上的老化时间	是
4	端口描述	用以向邻居发布本端口的IEEE 802局域网工作站规定的端口描述	否
5	系统名称	用以向邻居发布本地设备的系统名称	否
6	系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述	否
7	系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息	否
8	管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理	否
127	组织定义	允许不同的组织、软件和设备生产商定义向邻居设备发送信息的TLV	否

TLV一般分为两类，基本TLV和组织定义的TLV。

1) 基本TLV

基本TLV是实现LLDP协议必不可少的，它们包含网络管理的基本信息。

2) 组织定义的TLV

不同的组织定义了许多不同的TLV。端口VLAN ID、协议VLAN ID、VLAN名称以及协议标识TLV都是IEE 802.1定义的，MAC/PHY配置/状态、供电能力、链路聚合以及最大帧长度TLV则是由IEEE 802.3定义的。

注意:

要获取更多关于TLV的详细信息，请参考IEEE 802.1AB标准。

TP-LINK交换机中所支持的可携带TLV如下表所示：

端口描述	用以向邻居发布本端口的IEEE 802局域网工作站规定的端口描述。
系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息。
系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。
系统名称	用以向邻居发布本地设备的系统名称。
管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。
端口VLAN ID	用以向邻居发布本端口所处802.1Q VLAN的ID。
协议VLAN ID	用以向邻居发布本端口所处协议VLAN的ID。
VLAN名称	用以向邻居发布本端口所处VLAN被指派的名称。
链路聚合	用以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口ID。
MAC/PHY配置/状态	用以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。
最大帧长度	用以向邻居发布本端口的MAC和PHY支持的最大帧长度。
供电能力	用以向邻居发布本端口的基本供电信息。

表 16-1 TP-LINK 交换机中所支持的可携带 TLV

LLDP模块主要用来配置交换机的LLDP功能，包括**基本配置**、**设备信息**、**设备统计**和**LLDP-MED**四个部分。

16.1 基本配置

本功能包括**基本配置**和**端口配置**两个功能配置页面。

16.1.1 基本配置

配置交换机的LLDP功能，首先需要在本页配置交换机LLDP的全局功能和相关参数。

进入页面的方法：LLDP>>基本配置>>全局配置

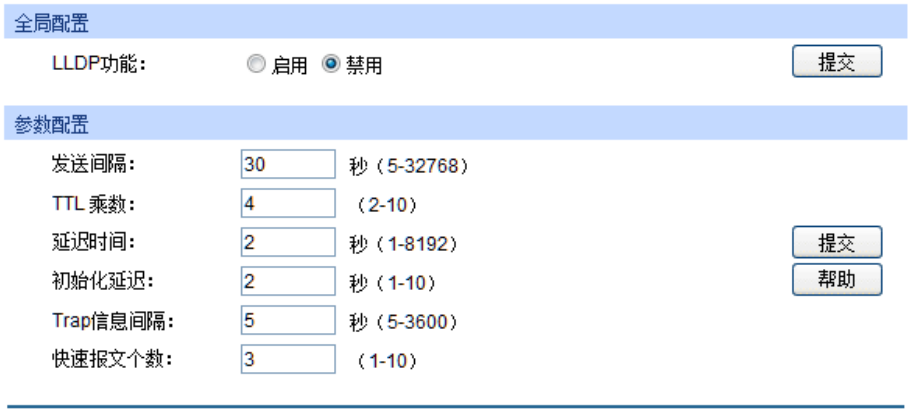


图 16-1 全局配置

条目介绍：

- **全局配置**

  LLDP功能: 选择是否启用LLDP。

- **参数配置**

  发送间隔: 配置本地设备向邻居设备发送LLDPDU的时间间隔。默认为30秒。

  TTL乘数: TTL乘数用以控制本地设备发送的LLDPDU中TTL字段的值，TTL即为本地信息在邻居设备上的存活时间。TTL=TTL乘数*发送间隔。默认值为4。

  延迟时间: 配置本地设备向邻居设备发送LLDPDU的延迟时间。当本地配置发生变化时，将延迟指定时间再发送LLDPDU通知邻居设备，从而可以避免由于本地配置频繁变化而导致LLDPDU的频繁发送。默认值为2秒。

  初始化延迟: 当端口LLDP工作模式改变时，将延迟一段时间再进行初始化，以避免端口LLDP工作模式频繁改变导致端口不断执行初始化。默认值为3秒。

  Trap信息间隔: 配置本地设备向网管系统发送Trap信息的发送时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致Trap信息的频繁发送。默认值为5秒。

快速报文个数: 当端口LLDP工作模式从禁用（或只接收）切换为发送接收（或只发送）时，为了让其它设备尽快发现本设备，将启用快速发送机制，即将LLDP报文的发送周期缩短为1秒，并连续发送指定数量的LLDPDU后再恢复为正常的发送周期。默认值为3个。

16.1.2 端口配置

在本页可以配置所有端口的LLDP参数。

进入页面的方法：**LLDP>>基本配置>>端口配置**

图 16-2 端口配置

条目介绍：

- **端口配置**

UNIT: 根据UNIT ID选择指定的交换机进行配置。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

端口状态: 选择端口的LLDP工作状态：

- 发送接收： 既发送也接收LLDPDU。
- 只接收：只对接收到的LLDPDU进行处理，而不向外发送LLDPDU。
- 只发送： 只向外发送LLDPDU，而不对接收到的LLDPDU进行处理。
- 禁用： 既不向外发送LLDPDU，也不对接收到的LLDPDU进行处理。

SNMP通知: 配置本端口是否启用SNMP通知。启用此功能时，如果发生trap事件，本地设备将会通知SNMP服务器。

TLV字段: 配置发送的LLDPDU中包含的TLV类型。

16.2 设备信息

本功能包括**本地信息**和**邻居信息**两个配置页面。

16.2.1 本地信息

在本页可以查看各端口的配置参数及系统参数。

进入页面的方法：**LLDP>>设备信息>>本地信息**

图 16-3 本地信息

条目介绍：

- **自动刷新**

自动刷新: 选择是否启用自动刷新功能。

刷新周期: 填写自动刷新的时间周期。默认为30秒。

本地信息: 根据UNIT ID点选指定交换机的端口查看端口和系统的配置信息。

16.2.2 邻居信息

在本页可查看邻居设备的信息。

进入页面的方法：**LLDP>>设备信息>>邻居信息**

图 16-4 邻居信息

条目介绍：

- **自动刷新**

  自动刷新: 选择是否启用自动刷新功能。

  刷新速度: 填写自动刷新的时间周期。默认为30秒。

根据UNIT ID点选指定交换机的端口查看端口的邻居信息。

- **邻居信息**

  系统名称: 显示邻居的系统名称。

  Chassis ID: 显示邻居设备的Chassis ID值。

  系统描述: 显示邻居的系统描述信息。

  邻居端口: 显示连接到本地端口的邻居端口号。

  详细信息: 点击查看对应邻居信息的详细信息。

16.3 设备统计

在本页可以查看本地设备LLDP相关统计信息。

进入页面的方法：**LLDP>>设备统计>>统计信息**

图 16-5 统计信息

条目介绍：

- **自动刷新**

  自动刷新： 选择是否启用自动刷新功能。

  刷新周期： 填写自动刷新的时间周期。默认为30秒。

- **全局统计信息**

  更新时间： 显示此统计数据的更新时间。

  创建邻居数量： 显示最新更新时本地设备已经创建的邻居数量。

  删除邻居数量： 显示最新更新时本地设备已经删除的邻居数量。

  丢弃邻居数量： 显示最新更新时本地设备已经丢弃的邻居数量。

  老化邻居数量： 显示最新更新时本地设备上已经老化的邻居数量。

- **端口统计信息**

  UNIT： 根据UNIT ID选择查看指定交换机的统计信息。

  端口： 显示本地端口号。

  发送报文： 显示本端口已经发送的LLDPDU数量。

  接收报文： 显示本端口已经接收到的LLDPDU数量。

  丢弃报文： 显示本端口丢弃的LLDPDU数量。

错误报文： 显示本端口接收的错误LLDPDU数量。

老化邻居： 显示本端口连接的邻居设备中老化邻居的数量。

丢弃TLV： 显示本端口接收LLDPDU时，丢弃的TLV数量。

未知TLV： 显示本端口接收的LLDPDU中包含的未知TLV的数量。

16.4 LLDP-MED

LLDP-MED （Link Layer Discovery Protocol-Media Endpoint Discovery，用于媒体终端发现的链路层发现协议）是 LLDP 协议的一个扩展，它仅适用于 LLDP-MED 规定的网络连接设备和终端设备之间的交互。

LLDP-MED 包括**基本配置**、**端口配置**、**本地信息**和**邻居信息**四个页面。

16.4.1 基本配置

在本页可以配置本地设备的 LLDP-MED 参数。

进入页面的方法：**LLDP>> LLDP-MED >>基本配置**

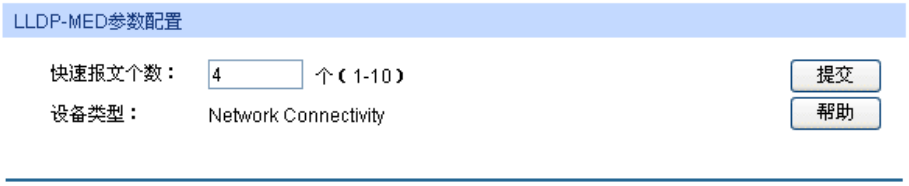


图 16-6 全局配置

条目介绍：

- **LLDP-MED 参数配置**

快速报文个数： 当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU，其默认值为 4。

设备类型： LLDP-MED 规定了两种设备类型，分别是网络连接设备（Network Connectivity Device）和终端设备（Endpoint Device），其中终端设备又可以分为 I、II 和 III 型共三种。交换机是一种网络连接设备。

16.4.2 端口配置

在本页可以配置所有端口的 LLDP-MED 状态和 TLV。

进入页面的方法：**LLDP>> LLDP-MED >>端口配置**

图 16-7 端口配置

条目介绍：

- **LLDP-MED 端口配置**

UNIT： 根据 UNIT ID 选择特定的交换机进行配置。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

LLDP-MED 状态： 启用/禁用端口的 LLDP-MED 功能。

- 启用：启用端口的 LLDP-MED 功能，同时端口的 LLDP 状态会被设置为发送接收。
- 禁用：禁用端口的 LLDP-MED 功能。

TLV 字段： 选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 信息。

点击<详细>按键即可进入如下页面，在本页可以配置端口发送的LLDPDU中包含的可选LLDP-MED的TLV。

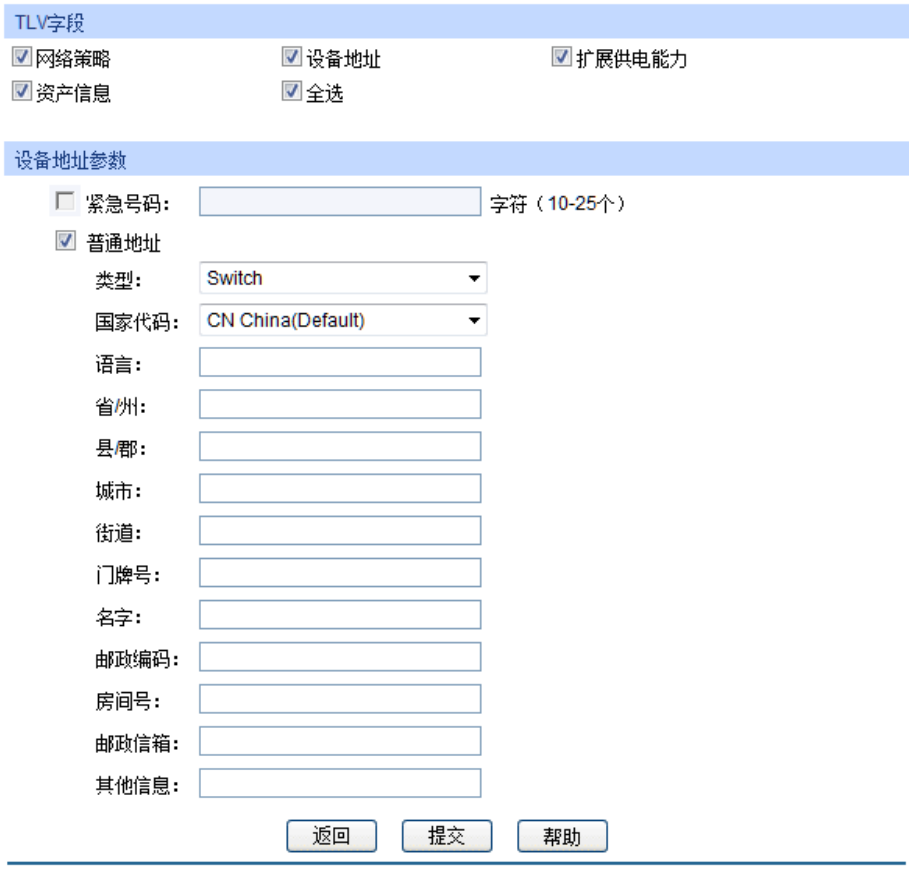


图 16-8 TLV 字段

条目介绍：

- **TLV 字段**

  网络策略： 网络策略 TLV 允许网络连接设备和终端设备发布本端口的 VLAN 配置与二层和三层属性。

  设备地址： 设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。您可以在**设备地址参数**中配置设备端口的详细地址。如果没有配置**设备地址参数**而又包含了设备地址 TLV，那么将会使用一个默认的地址信息。

  扩展供电能力： 扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交互详细的供电信息，例如供电优先级、供电状态等

  资产信息： 资产信息中包含七种基本的资产信息 TLV，分别为硬件版本 TLV、固件版本 TLV、软件版本 TLV、序列号 TLV、制造厂商名称 TLV、模块名称 TLV 和资产跟踪 ID TLV。

- **设备地址参数**

  紧急号码： 紧急号码是紧急呼叫服务使用的号码，用以呼叫 CAMA 或者 PSAP，字符长度介于 10 到 25 之间。

设备地址： 普通地址使用 IETF 规定的地址信息格式。

- 类型：描述本地设备充当的设备角色，当前有三种选择：DHCP 服务器，switch 和 LLDP-MED 终端。
- 国家代码：ISO 3166 规定的代表国家的两个字符的代码，例如 CN、US 等。
- 语言、省/州等：普通地址的详细信息。

16.4.3 本地信息

在本页可以查看所有端口的 LLDP-MED 配置信息。

进入页面的方法：**LLDP>> LLDP-MED >>本地信息**

图 16-9 本地信息

条目介绍：

➢ **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为 30 秒。

➢ **LLDP-MED 本地信息**

根据 UNIT ID 切换交换机，并点选特定端口查看本地信息。

本地端口： 显示本地端口号。

设备类型： 显示 LLDP-MED 规定的本地设备类型。

应用类型： 显示本地设备支持的各种应用。

媒体策略未知标记： 显示网络策略 TLV 中包含的未知标记位设置。

VLAN tagged： 显示应用所需 VLAN Tag 类型：tagged 或者 untagged。

VLAN ID： 显示端口所处 802.1Q VLAN 的 ID 值。

二层优先级： 显示特定应用使用的二层优先级。

QOS DSCP 值： 显示特定应用使用的 DSCP 值。

16.4.4 邻居信息

在本页可以查看所有端口邻居的 LLDP-MED 信息。

进入页面的方法：**LLDP>> LLDP-MED >>邻居信息**

图 16-10 邻居信息

条目介绍：

- **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为 30 秒。

- **邻居信息**

根据 UNIT ID 切换交换机，并点选特定端口查看本地信息。

设备类型： 显示邻居设备的 LLDP-MED 设备类型。

应用类型： 显示邻居设备的应用类型。

设备地址类型： 显示邻居设备的地址类型。

供电类型： 显示邻居设备的供电设备类型。

查询： 查看更详细的邻居 LLDP-MED 信息。

回目录

第17章 集群管理

随着网络技术的发展，网络的规模越来越大，网络设备的数量越来越多，所以网络管理也就越来越烦琐。数量众多的设备需要分配不同的网络地址，每台管理设备均需要单独配置之后才能够满足应用的需要，以上这些造成管理人员很大的压力。

集群管理可以很好地解决上述问题。集群是可以当作单一设备来管理的一组网络设备的集合，集群管理的主要目的是解决大量分散的网络设备的集中管理问题。网络管理者通过集群中的一个交换机就可以实现对集群中其它交换机的管理和维护；其中执行管理功能的交换机是命令交换机，其它被管理的交换机是成员交换机，命令交换机和成员交换机组成了一个“集群”。典型组网应用如图 17-1 所示。

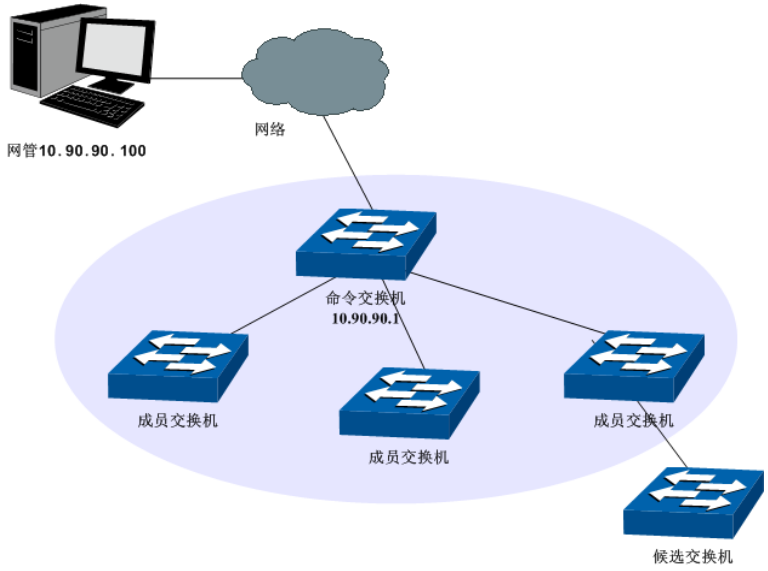


图 17-1 集群典型应用组网图

- **集群角色**

由于各个交换机在集群中所处的地位和功能的不同，形成了不同的角色，您可以配置交换机在集群中的角色。集群的角色有三种：

命令交换机：在集群中，唯一的可以配置和管理整个集群的交换机。命令交换机通过收集NDP（Neighbor Discovery Protocol，邻居发现协议）和NTDP（Neighbor Topology Discovery Protocol，邻居拓扑发现协议）信息来发现和确定候选交换机。

成员交换机：集群中被管理的交换机。

候选交换机：具有加入集群能力，但还没有加入任何集群的交换机。

独立交换机：未启用集群功能的交换机。

各种集群角色可以按一定的规则进行转换：

- 用户在交换机上创建集群的同时，将当前交换机指定为命令交换机。
- 命令交换机通过收集相关信息，发现和确定候选交换机。
- 候选交换机加入集群后，成为成员交换机。
- 集群内的成员交换机被删除后将恢复为候选交换机。
- 命令交换机只有在删除集群时才能恢复为候选交换机。

➢ **集群工作原理**

集群通过NDP、NTDP、CMP（Cluster Management Protocol，集群管理协议）三个协议，对集群内部的交换机进行配置和管理。

集群的过程分为拓扑发现、拓扑收集和集群的建立维护，具体工作过程如下：

- 拓扑发现：所有交换机通过NDP 来获取邻居交换机的信息。
- 拓扑收集：命令交换机通过NTDP 来收集网络内指定跳数范围内的交换机信息以及各个交换机的连接信息，并从收集到的拓扑信息中确定集群的候选交换机。
- 集群建立维护：命令交换机根据NTDP 收集到的候选设备信息完成将候选交换机加入集群、成员交换机离开集群等集群管理操作。

集群管理模块主要用于配置交换机的集群管理功能，包括**拓扑发现**、**拓扑收集**以及**集群管理**三个部分。

17.1 拓扑发现

集群中的交换机使用NDP来获取与其直接相连的邻居交换机的信息。交换机周期性地向邻居发送NDP报文，同时也会接收但不转发邻居交换机发送的NDP报文。NDP报文中包含NDP信息（包括本交换机的名称、MAC地址、软件版本等信息）等。

交换机会存储和维护一个邻居信息表，邻居信息表里包含每个邻居交换机的NDP信息表项。如果交换机收到新邻居的NDP信息，则会在邻居信息表新增一个表项；如果从邻居交换机收到的NDP信息与旧的信息不同，则更新邻居信息表中的数据，如果相同，则只更新老化时间，如果超过老化时间还没有收到邻居发送的NDP信息，将自动删除相应的邻居表项。

本功能包括**邻居信息**、**配置显示**和**全局配置**三个配置页面。

17.1.1 邻居信息

在本页可以查看交换机的NDP邻居信息表。

进入页面的方法：集群管理>>拓扑发现>>邻居信息

图 17-2 邻居信息

条目介绍：

➢ **邻居查找**

查找选项： 选择欲查找条目需包含的信息。

➢ **邻居信息**

本地端口： 显示本交换机的端口号。

远程端口： 显示与相应端口相连的邻居交换机的端口号。

设备名称： 显示邻居交换机的名称。

设备MAC： 显示邻居交换机的MAC地址。

软件版本： 显示邻居交换机的软件版本。

老化时间： 显示邻居交换机发送的NDP报文在本交换机上的剩余时间。

17.1.2 配置显示

在本页可以查看交换机的NDP配置信息。

进入页面的方法：集群管理>>拓扑发现>>配置显示

图 17-3 配置显示

条目介绍：

- **全局配置**

NDP状态： 显示本交换机的全局NDP状态。

老化定时器： 显示本交换机发送的NDP报文在邻居交换机上的老化时间。

Hello定时器： 显示本交换机NDP报文发送的间隔时间。

- **端口状态**

UNIT： 根据UNIT ID选择查看特定交换机的信息。

端口： 显示交换机的端口号。

NDP状态： 显示当前端口的NDP状态。

发送NDP包数： 显示端口当前发送的NDP数据包数。

接收NDP包数： 显示端口当前接收的NDP数据包数。

错误NDP包数： 显示端口当前接收到的错误NDP数据包数。

邻居数： 显示端口所连接的邻居交换机数。

LAG： 显示端口所属的LAG组。

详细信息： 点击此按键，将显示该端口的收集到的邻居信息。

清除： 清楚端口的报文统计信息，或点击底部的<清除>按键清除所有统计信息。

17.1.3 全局配置

在本页可以配置交换机的NDP功能。

进入页面的方法：集群管理>>拓扑发现>>全局配置

图 17-4 全局配置

条目介绍：

- **全局配置**

NDP状态：	选择是否启用全局NDP功能。
老化定时器：	填写本交换机发送的NDP报文在接收设备上的老化时间。默认为180秒。
Hello定时器：	填写本交换机NDP报文发送的时间间隔。默认为60秒。

- **端口状态**

根据 UNIT ID 切换交换机，并点选特定端口配置端口的 NDP 特性，选中端口并提交保存后，端口将使能 NDP 特性。

注意：

- 必须在全局配置和端口状态中同时启用NDP状态，NDP功能才能正常运行。
- 老化定时器时间要大于Hello定时器时间，否则将引起NDP端口邻居信息表的不稳定。

17.2 拓扑收集

NTDP用于命令交换机收集整个网络指定跳数的拓扑信息。NTDP 根据NDP邻居信息表发送和转发NTDP 拓扑收集请求，收集指定跳数内的网络中每个交换机的NDP 信息及其连接信息。命令交换机可以定时在网络内进行拓扑收集，您也可以随时在命令交换机上手动启用拓扑收集。

命令交换机发送拓扑收集请求报文后，大量交换机会同时收到拓扑收集请求并同时发送拓扑收集响应报文，如此以来可能造成网络拥塞和命令交换机负担过重。为了避免上述现象的产生，设计了两个时间参数来控制拓扑收集请求报文扩散速度：

- 请求跳数延迟时间：交换机收到拓扑收集请求，会等待该时间段之后，才开始在第一个启用NTDP的端口转发该拓扑收集请求报文。
- 端口跳数延迟时间：在同一个交换机上，除第一个端口外，每个启用NTDP 功能的端口在前一个端口发送拓扑收集请求报文后，都会等待该时间段，再进行拓扑收集请求报文的转发。

本功能包括**设备列表**、**配置显示**和**全局配置**三个配置页面。

17.2.1 设备列表

在此处可以查看NTDP收集到的设备信息。同时，无论集群是否建立，您都可以在本页随时手动收集NTDP 信息，从而更有效地对设备进行实时管理与监控。

进入页面的方法：集群管理>>拓扑收集>>设备列表

图 17-5 设备列表

条目介绍：

- **设备信息列表**

设备名称： 显示NTDP所收集到的设备名称。

设备MAC： 显示该设备的MAC地址。

集群名： 显示该设备的集群名称。

角色： 显示该设备在集群中的角色。

- Commander：配置并管理集群的交换机。
- Member：在集群中被管理的交换机。
- candidate：能够成为集群成员但是还未加入集群的交换机。
- Individual：未启用集群功能的交换机。

跳数： 显示该设备距离本交换机的跳数。

邻居信息： 点击<详细信息>，可以查看该设备的详细信息及其邻居信息表。

点击<详细信息>按键后，可以看到NDTP收集到的设备信息。

图 17-6 当前设备信息

17.2.2 配置显示

在本页可以查看交换机的NTDP配置信息。

进入页面的方法：集群管理>>拓扑收集>>配置显示

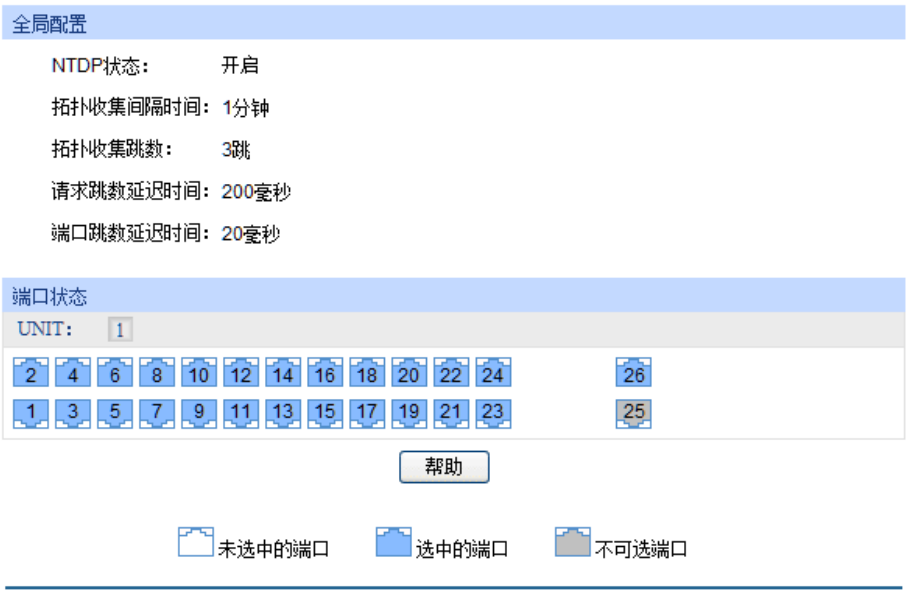


图 17-7 配置显示

条目介绍：

- **全局配置**

  NTDP状态： 显示本交换机的全局NTDP状态。

  拓扑收集间隔时间： 显示本交换机拓扑信息收集的周期。

  拓扑收集跳数： 显示本交换机拓扑收集的范围。

  请求跳数延迟时间： 显示本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。

  端口跳数延迟时间： 显示本交换机在相邻端口转发拓扑请求报文的延时时间。

- **端口状态**

显示当前端口的NTDP状态，蓝色表示端口的NTDP特性已使能。

17.2.3 全局配置

在本页可以配置交换机的NTDP功能。

进入页面的方法：集群管理>>拓扑发现>>全局配置

图 17-8 全局配置

条目介绍：

- **全局配置**

NTDP状态：	选择是否启用全局NTDP功能。
拓扑收集间隔时间：	填写本交换机拓扑信息收集的周期。默认为1分钟。
拓扑收集跳数：	填写本交换机拓扑收集的范围。默认为3跳。
请求跳数延迟时间：	填写本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。默认为200毫秒。
端口跳数延迟时间：	填写本交换机在相邻端口转发拓扑请求报文的延时时间。默认为20毫秒。

- **端口状态**

根据UNIT ID切换交换机，并点选特定端口配置端口的NTDP特性，选中端口并提交保存后，端口将使能NTDP特性。

注意：

- 必须在全局配置和端口状态中同时启用NTDP状态，NTDP功能才能正常运行。

17.3 集群管理

命令交换机通过NDP 和NTDP 协议发现和确定候选交换机，并将候选交换机自动加入集群，您也可以通过手动配置将候选交换机加入到集群中。候选交换机成功加入集群后，将获得由命令交换机为它分配的私有IP 地址。您可以在命令交换机上直接访问成员交换机的Web页面，对成员交换机进行管理。

本功能包括**配置显示**、**集群配置**、**成员管理**和**拓扑图**四个配置页面。

17.3.1 配置显示

在本页可以查看到当前集群的状态。

进入页面的方法：集群管理>>集群管理>>配置显示

- 当前交换机为候选交换机时，可以看到：

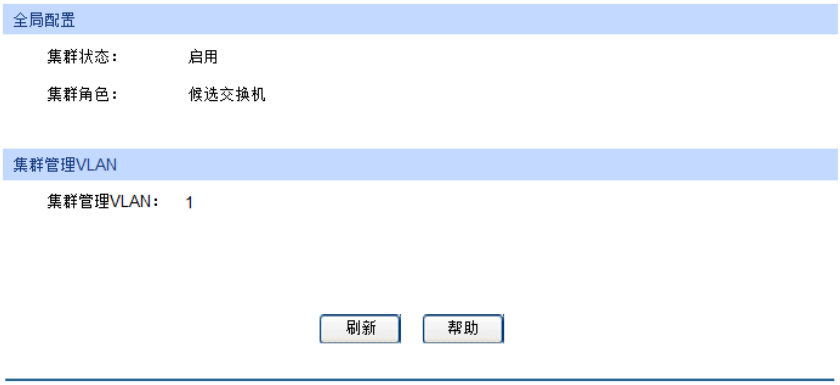


图 17-9 候选交换机的配置显示

条目介绍：

- **全局配置**

  集群状态： 显示当前交换机的集群状态。

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  集群管理VLAN： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- 当前交换机为命令交换机时，可以看到：

图 17-10 命令交换机的配置显示

条目介绍：

- **全局配置**

  集群状态： 显示当前交换机的集群状态。

  集群角色： 显示交换机在集群中的角色。

  集群名： 显示交换机当前的集群名称。

- **集群管理VLAN**

  集群管理VLAN： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- **集群设置**

  集群地址池、掩码： 显示集群中成员交换机的私有IP地址范围。

  保持时间： 显示集群信息在命令交换机中保存的时间。

  时间间隔： 显示本交换机与成员交换机握手报文的时间间隔。

- **成员信息**

  设备名称： 显示成员交换机的名称。

  设备MAC： 显示成员交换机的MAC地址。

  IP地址： 显示成员交换机在集群中的IP地址。

  状态： 显示成员交换机的连通性。

  角色： 显示交换机当前的集群角色。

  加入集群时间： 显示成员交换机加入集群的时间。

  跳数： 显示成员交换机距离命令交换机的跳数。

- 当前交换机为成员交换机时，可以看到：

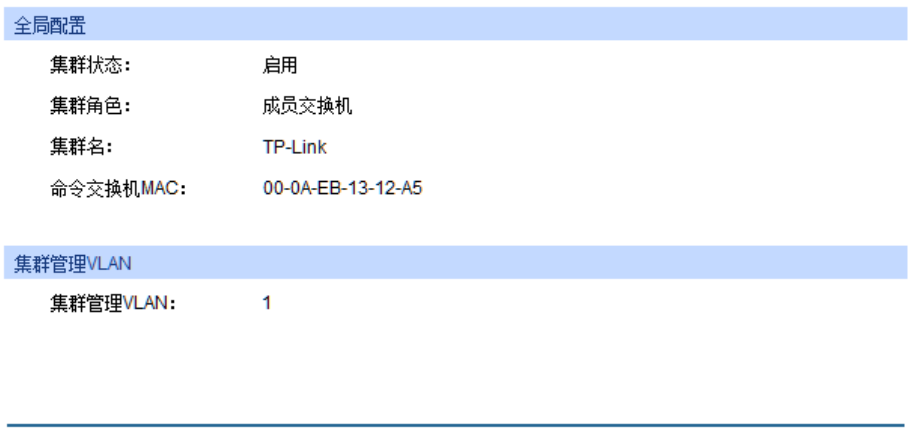


图 17-11 成员交换机的配置显示

条目介绍：

- **全局配置**

  集群状态： 显示当前交换机的集群状态。

  集群角色： 显示交换机在集群中的角色。

  集群名： 显示交换机当前的集群名称。

  命令交换机MAC： 显示命令交换机的MAC地址。

- **集群管理VLAN**

  集群管理VLAN： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- 当前交换机为独立交换机时，可以看到：

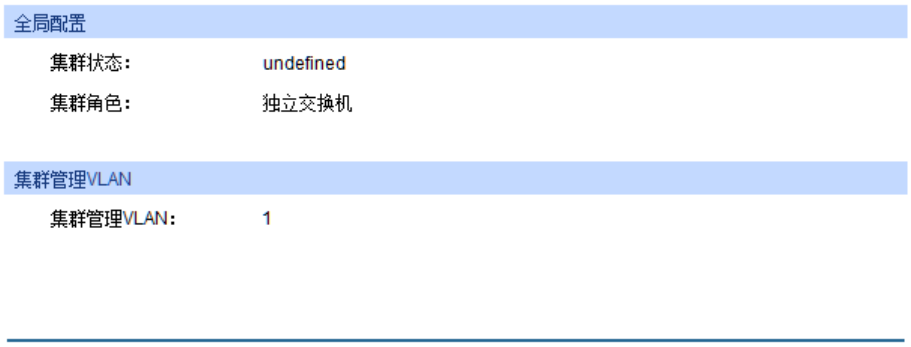


图 17-12 独立交换机的配置显示

条目介绍：

- **全局配置**

  集群状态： 显示当前交换机的集群状态。

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  集群管理VLAN： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

17.3.2 集群配置

在本页可以配置交换机的集群状态。

进入页面的方法：集群管理>>集群管理>>集群配置

- 当前交换机为候选交换机时，可以看到：

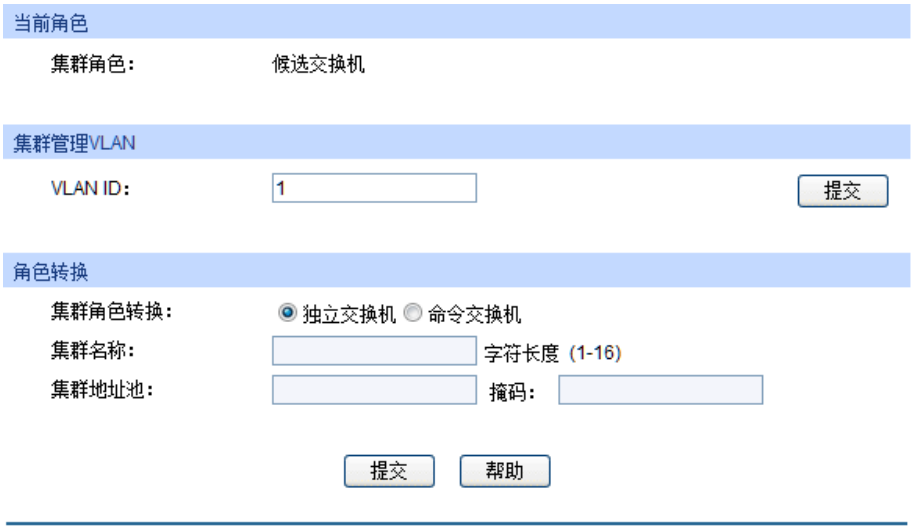


图 17-13 候选交换机的集群配置

条目介绍：

- **当前角色**

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  VLAN ID： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- **角色转换**

  独立交换机： 将交换机的集群角色转换为独立交换机。

  命令交换机： 将交换机的集群角色转换为命令交换机。之后，您还需要配置集群的基本属性：

  - 集群名称：配置交换机当前的集群名称。
  - 集群地址池、掩码：配置集群中成员交换机的私有IP地址范围。

- 当前交换机为命令交换机时，可以看到：

图 17-14 命令交换机的集群配置

条目介绍：

- **当前角色**

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  VLAN ID： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- **角色转换**

  候选交换机： 将交换机的集群角色转换为候选交换机。

- **集群配置**

  保持时间： 填写集群信息在命令交换机中保存的时间。取值范围1-255秒，默认为20秒。

  时间间隔： 填写命令交换机与成员交换机握手报文的时间间隔。取值范围1-255秒，默认为20秒。

- 当前交换机为成员交换机时，可以看到：

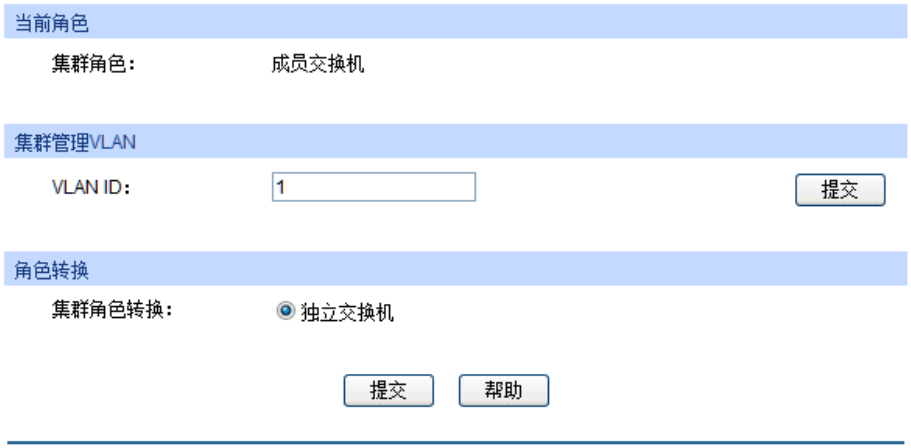


图 17-15 成员交换机的集群配置

条目介绍：

- **当前角色**

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  VLAN ID： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- **角色转换**

  独立交换机： 将交换机的集群角色转换为独立交换机。

- 当前交换机为独立交换机时，可以看到：

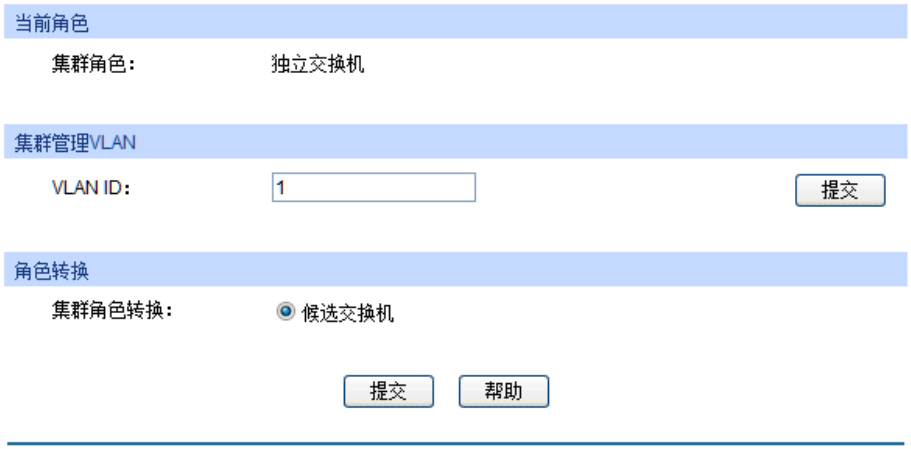


图 17-16 独立交换机的集群配置

条目介绍：

- **当前角色**

  集群角色： 显示交换机在集群中的角色。

- **集群管理VLAN**

  VLAN ID： 可以进行集群管理的VLAN，只在集群中用到。这种VLAN只有一个，必须是有端口的并且已经配置了IP的VLAN。删除VLAN或者删除VLAN的interface的时候要先判断该VLAN有没有建立集群，如果有，请先删除集群或者修改集群的管理VLAN为别的VLAN，管理VLAN的默认值为1。

- **角色转换**

  候选交换机： 将交换机的集群角色转换为候选交换机。

17.3.3 成员管理

当交换机为集群中的命令交换机时，可以在命令交换机上手动指定要加入集群的候选交换机，也可以手动删除集群中指定的成员交换机，同时也可以在本页对成员交换机进行配置管理。

进入页面的方法：集群管理>>集群管理>>成员管理

图 17-17 成员管理

条目介绍：

- **手动成员加入**

  成员MAC： 填写候选交换机的MAC地址。

- **成员信息**

  选择： 勾选条目进行管理或删除操作。

  设备名称： 显示成员交换机的名称。

  设备MAC： 显示成员交换机的MAC地址。

  IP地址： 显示成员交换机在集群中的IP地址。

  状态： 显示成员交换机的连通性。

  角色： 显示交换机当前的集群角色。

  加入集群时间： 显示成员交换机加入集群的时间。

跳数： 显示成员交换机距离本交换机的跳数。

管理： 勾选条目后点击此按键，进入相应的成员交换机的Web页面。

17.3.4 拓扑图

在本页可以看到集群的整个拓扑结构图，也可以点击节点交换机直接进入相应的管理页面，从而对该交换机进行配置管理。同时双击拓扑图上的各个节点交换机，可以看到该交换机的详细信息。

进入页面的方法：集群管理>>集群管理>>拓扑图

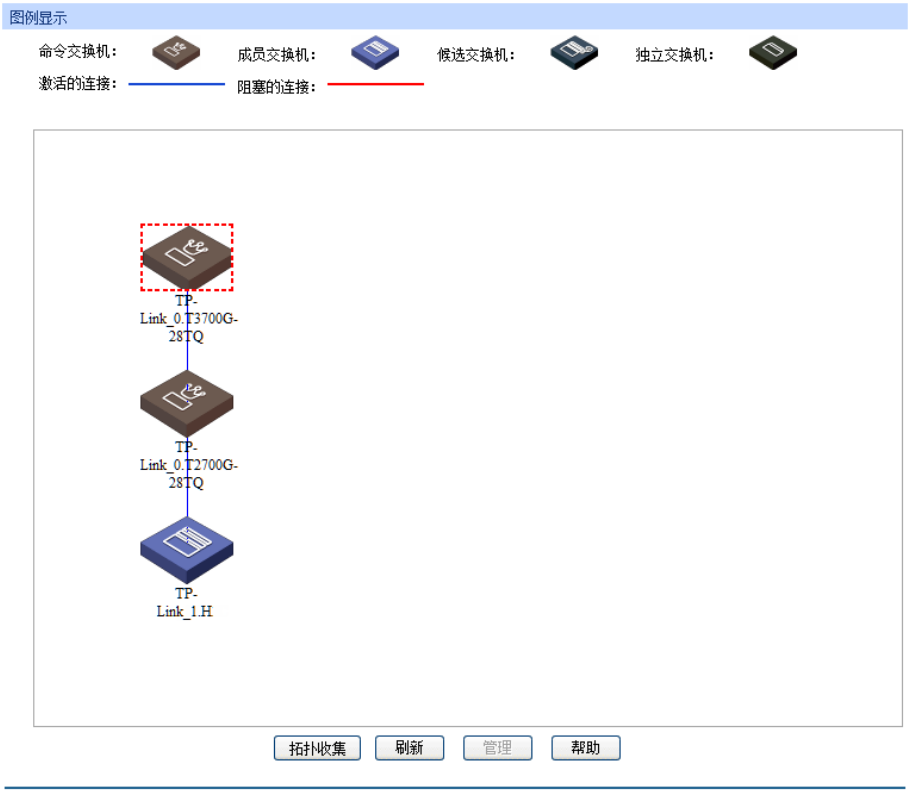


图 17-18 拓扑图

条目介绍：

- **图例显示**

拓扑收集： 点击此按键后将集群内的拓扑信息以拓扑图的形式展现出来。

管理： 如果当前设备为集群中的命令交换机，并且选中的设备为此集群中的成员交换机，那么点击此按键，将进入相应交换机的管理页面。

集群管理功能全局配置步骤：

在配置集群之前，首先您需要明确集群内各交换机的角色及功能，做好集群的规划工作。

- 若此交换机为命令交换机：

步骤	操作	说明
1	启用NDP功能，并配置NDP参数	可选操作。在**集群管理>>拓扑发现>>全局配置**页面，启用交换机的NDP功能。

步骤	操作	说明
2	启用NTDP功能，并配置NTDP参数	可选操作。在**集群管理>>拓扑收集>>全局配置**页面，启用交换机的NTDP功能。
3	建立集群，并配置集群参数	可选操作。在**集群管理>>集群管理>>集群配置**页面，建立集群并配置集群参数。
4	管理集群设备	可选操作。 在**集群管理>>集群管理>>成员管理**页面，选择成员交换机，点击<管理>按键，即可进入该成员交换机的Web页面进行管理。 也可在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机的图标，点击<管理>按键，即可进入该成员交换机的Web页面进行管理。

- 若此交换机为成员交换机：

步骤	操作	说明
1	启用NDP功能	可选操作。在**集群管理>>拓扑发现>>全局配置**页面，启用全局和端口的NDP功能。
2	启用NTDP功能	可选操作。在**集群管理>>拓扑收集>>全局配置**页面，启用全局和端口的NTDP功能。
3	手动收集拓扑信息	可选操作。 在**集群管理>>拓扑收集>>设备列表**页面，点击<拓扑收集>按键，手动收集拓扑信息。 也可在**集群管理>>集群管理>>拓扑图**页面，点击<拓扑收集>按键，手动收集拓扑信息。
4	查询集群中其它交换机的详细信息	在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息。

17.4 集群管理功能组网应用

- **组网需求**

三台交换机构成一个集群，其中：一台为命令交换机（以我司交换机T3700G-28TQ为例）、其它交换机为成员交换机。网管通过命令交换机来管理整个集群。

- 命令交换机的端口1/0/1与外网连接，端口1/0/2、端口1/0/3分别与成员交换机1、成员交换机2连接。
- 集群地址池：175.128.0.1；掩码：255.255.255.0 。

➢ **组网图**

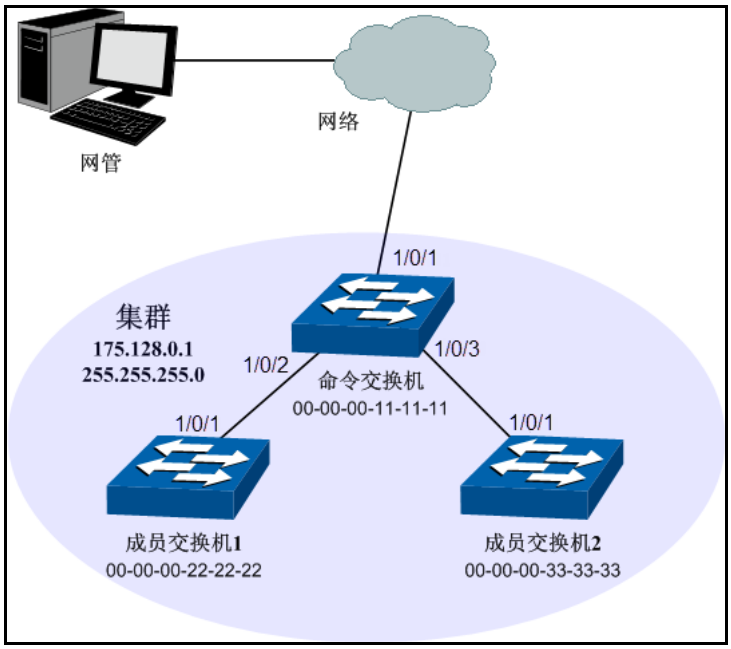


图 17-19 集群管理组网图

➢ **配置步骤**

- 配置成员交换机

步骤	操作	说明
1	启用NDP功能	在**集群管理>>拓扑发现>>全局配置**页面，启用全局和端口1/0/1的NDP功能。
2	启用NTDP功能	在**集群管理>>拓扑收集>>全局配置**页面，启用全局和端口1/0/1的NTDP功能。

- 配置命令交换机

步骤	操作	说明
1	启用NDP功能	在**集群管理>>拓扑发现>>全局配置**页面，启用全局和端口1/0/2、1/0/3的NDP功能。
2	启用NTDP功能	在**集群管理>>拓扑收集>>全局配置**页面，启用全局和端口1/0/2、1/0/3的NTDP功能。
3	建立集群，配置集群参数	在**集群管理>>集群管理>>集群配置**页面，配置集群角色为命令交换机，并填写集群信息。 集群地址池：175.128.0.1 掩码：255.255.255.0
4	配置成员交换机	在**集群管理>>集群管理>>成员管理**页面，选择成员交换机，点击<管理>按键，进入该交换机的Web页面。 也可在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机图标，点击<管理>按键，可以进入该交换机的Web页面。

回目录

第18章　系统维护

系统维护模块将管理交换机的常用系统工具组合在一起，为定位并排除交换机和网络故障提供便捷的方法。

1)　运行状态：对交换机内存和CPU进行监控。

2)　系统日志：通过系统日志查看在交换机上的配置参数并找出错误的配置。

3)　系统诊断：检测与交换机连接的线缆及对端设备的可用性。

4)　网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。

18.1　运行状态

在本功能中可以通过曲线数据监控交换机CPU和内存的使用情况，CPU和内存使用率应该在一定数值上下波动。当CPU和内存使用率波动较大且明显增大时，请检查网络是否受到攻击。

本功能包括**CPU监控**和**内存监控**两个配置页面。

18.1.1 CPU监控

进入页面的方法：系统维护>>运行状态>>CPU监控

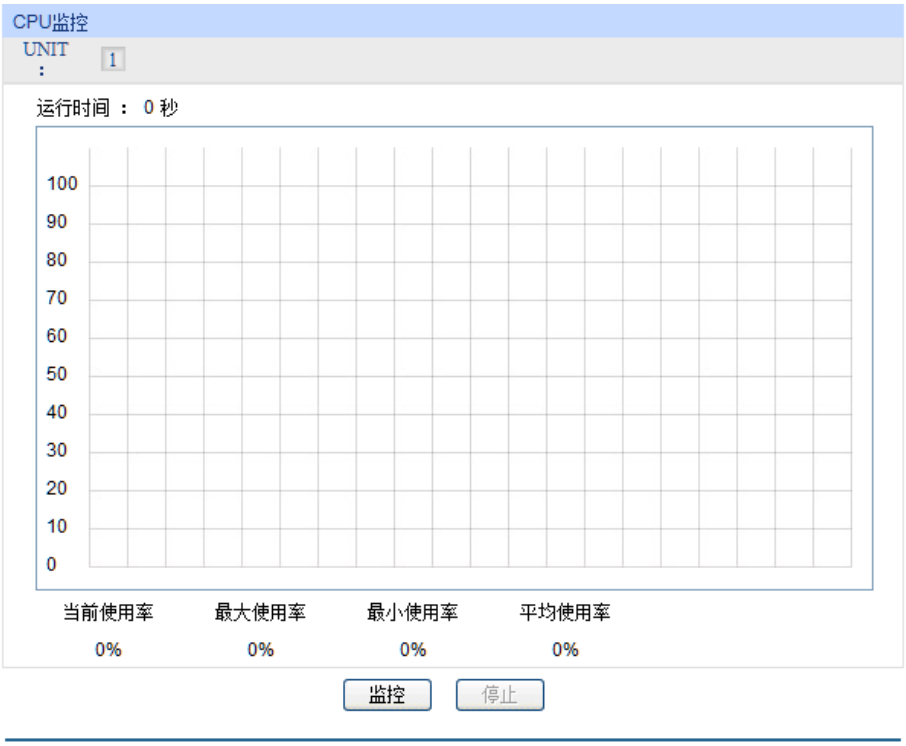


图 18-1 CPU监控

点击<监控>按键，图 18-1 所示页面会每隔 4 秒反馈一次监控数值，显示交换机 CPU 使用率。

18.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

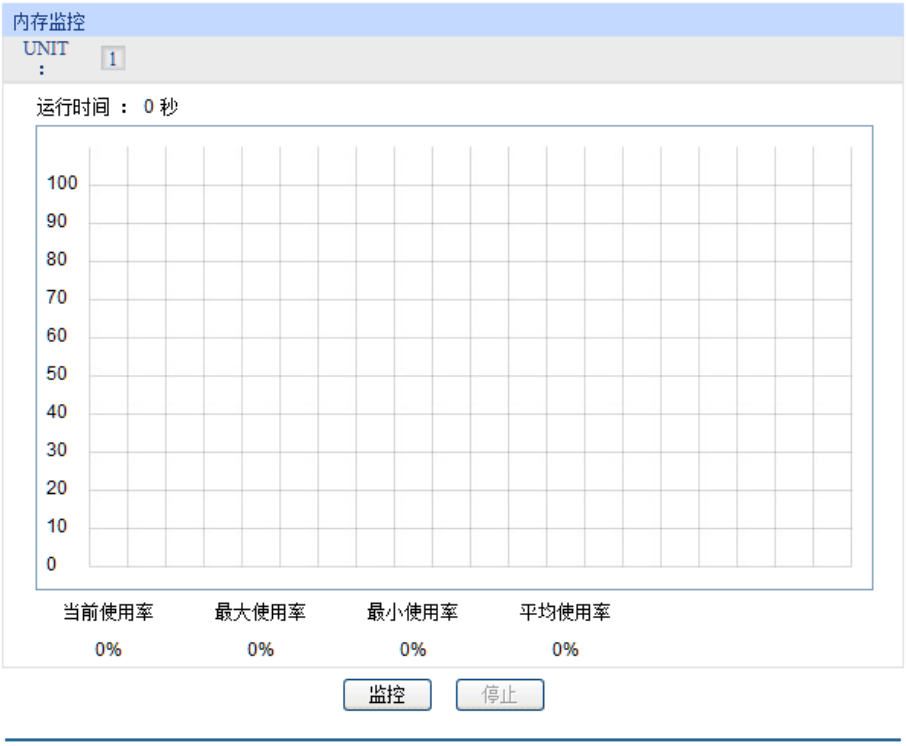


图 18-2 内存监控

点击<监控>按键，图 18-2所示页面会每隔4秒反馈一次监控数值，显示交换机内存使用率。

18.2 系统日志

本交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。

本交换机的系统日志分为八个等级，如表 18-1所示。

级别名称	等级	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debugging	7	调试过程产生的信息

表 18-1 日志等级

本功能包括**日志列表**、**本地日志**、**远程日志**和**日志导出**四个功能页面。

18.2.1 日志列表

系统日志可以保存到两个不同的地方：日志缓冲区和日志文件。日志缓冲区的日志信息在交换机重启后将会丢失，日志文件里的日志信息在交换机重启后仍然有效。日志列表显示了日志缓冲区中的系统日志信息。

进入页面的方法：系统维护>>系统日志>>日志列表

图 18-3 日志列表

条目介绍：

- **系统日志列表**

UNIT：	根据UNIT ID选择查看特定交换机的日志信息。
序号：	显示该日志信息的序号。
时间：	显示该日志信息的发生时间。需先在**系统管理>>系统配置>>系统时间**页面进行配置后，系统日志才能获取到正确的时间。
模块名：	显示该日志信息所属功能模块，从下拉列表可选择显示某一模块的日志信息。
严重级别：	显示该日志信息的严重级别，从下拉列表选择某一级别，可显示小于或等于该级别值的日志信息。
日志信息：	显示该日志信息的内容。

注意：

- 严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。
- 本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为1024条。

18.2.2 本地日志

本地日志是指保存在本交换机上的所有系统日志信息。在缺省情况下，所有的系统日志将保存到日志缓冲区。在此页面中可以对日志的存储区进行配置，选择将日志保存到日志缓冲区或者日志文件。

进入页面的方法：系统维护>>系统日志>>本地日志

图 18-4 本地日志

条目介绍：

- **本地日志配置**

选择： 勾选相应的日志记录位置进行配置。

日志缓冲区： **日志列表**页面上显示的即为缓冲区中的信息，在断电重启后这些信息将会丢失。

日志文件： 日志文件中的日志信息在断电重启后不会丢失，可通过导出日志文件来查看。默认未启用。

严重级别： 限定各个输出方向上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会进行记录。

状态： 启用/禁用保存到该位置的日志功能。

18.2.3 远程日志

远程日志功能可以将本交换机的系统日志发送到日志服务器上。日志服务器相当于一个可维护的共享消息区，它可以对网络中各设备产生的日志信息进行集中的监控和管理。

TP-LINK日志服务器提供了一个用于日志监视、存储和管理的窗口系统，并提供自动备份的功能。日志格式遵循RFC3164标准，**TP-LINK**日志服务器的安装过程及操作方法请登录我司官方网站**http://www.tp-link.com.cn**下载安装软件和操作指南。

进入页面的方法：系统维护>>系统日志>>远程日志

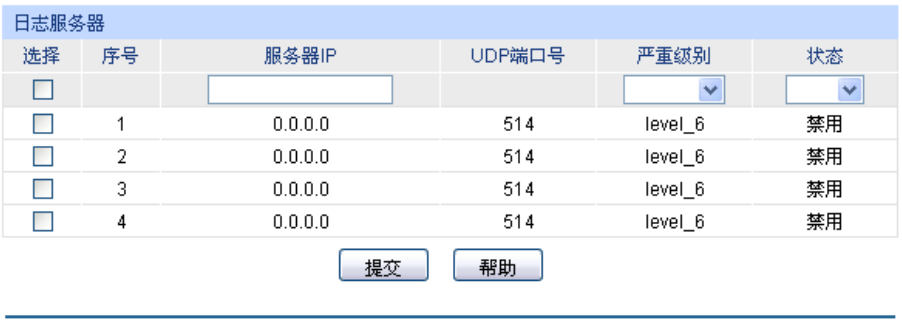


图 18-5 日志服务器

条目介绍：

- **日志服务器**

选择： 勾选相应的日志服务器进行配置。

序号：	日志服务器序号。本交换机共支持4个日志服务器。
服务器IP：	配置日志服务器的IP地址。
UDP端口号：	发送/接收系统日志时所用到的UDP端口号，这里使用标准的514端口。
严重级别：	限定发往各个服务器上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会发送到相应的服务器。
状态：	启用/禁用该服务器。

18.2.4 日志导出

日志导出功能可以将保存在交换机里的日志信息以文件的形式导出，作为设备诊断和统计分析之用。尤其在发生严重错误导致系统崩溃时，可在重启后导出日志信息，以获取相关的一些重要信息，为诊断设备提供支持。

进入页面的方法：系统维护>>系统日志>>日志导出

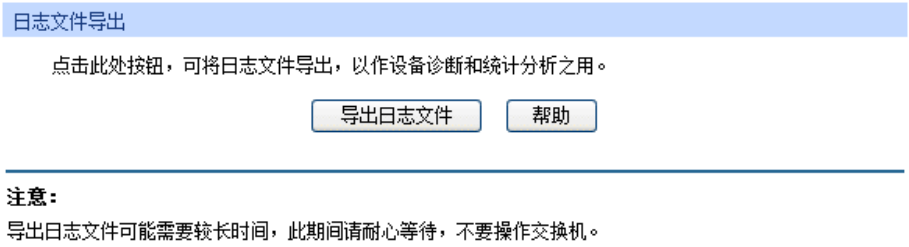


图 18-6 日志导出

条目介绍：

- **日志文件导出**

导出日志文件：	点击此按键导出日志文件中的日志信息。

18.3 系统诊断

本交换机提供了线缆检测和环回检测功能。

18.3.1 线缆检测

线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

进入页面的方法：系统维护>>系统诊断>>线缆检测

图 18-7 线缆检测

条目介绍：

- **检测端口**

根据 UNIT ID 切换交换机，并点选特定端口，选中端口并提交后，将自动进行线缆检测。

- **检测结果**

线对： 显示线对序号。

线路状态： 检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。

- 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。
- 短路：线路金属内芯互相接触，导致短路。
- 阻抗失配：网线质量问题。

线路长度： 若线路为正常状态，显示该线缆的长度范围。

出错长度： 若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

注意：

- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

18.3.2 环回检测

环回检测可以在不依赖外部设备的情况下检查端口是否可用，同时可以检测对端设备的可用性，有助于确定和解决网络故障，能够迅速方便地定位网络故障。本交换机的环回检测分为内环检测和外环检测。

1) 内环检测：无须借助外部设备，即可检测交换机端口是否正常。

2) 外环检测：可以检测与交换机相连的对端设备是否正常，同时插入自环头还可以检测交换机的自身性能。自环头的做法是用网线将一个水晶头的1/3、2/6、4/7、5/8管脚成对短接即可。

进入页面的方法：系统维护>>系统诊断>>环回检测

图 18-8 环回检测

条目介绍：

- **检测类型**

检测类型：	选择要进行检测的类型。外环检测需要连接到外部设备或者自环头。
UNIT：	根据UNIT ID切换交换机，并点选特定端口，选中端口并提交后，将自动进行环回检测。

- **检测结果**

显示检测结果。

18.4 网络诊断

本交换机提供了Ping检测和Tracert检测功能。

18.4.1 Ping检测

Ping检测功能可以检测交换机与某网络设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping检测过程如下：

1) 交换机向目标设备发送ICMP请求报文；

2) 如果网络工作正常，则目标设备在接收到该报文后，向交换机返回ICMP应答报文；显示相关统计信息；

3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息。

进入页面的方法：系统维护>>网络诊断>>Ping检测

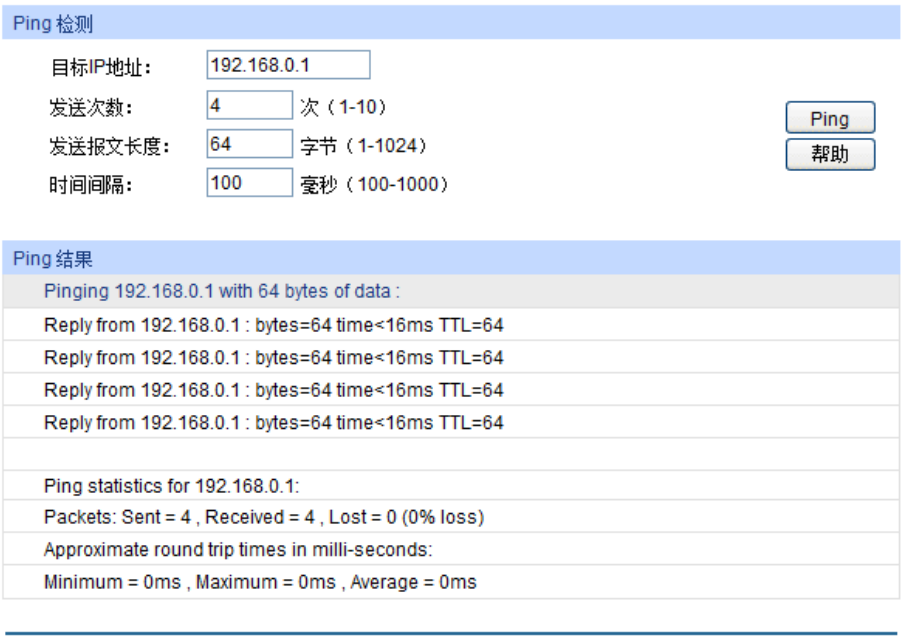


图 18-9 Ping检测

条目介绍：

- **Ping检测**

目标IP地址：	填写需要测试的目标节点的IP地址。
发送次数：	填写Ping检测时发送的检测包次数。建议使用缺省值。
发送报文长度：	填写Ping检测时发送的检测包长度。建议使用缺省值。
时间间隔：	发送ICMP 请求报文的时间间隔。

18.4.2 Tracert检测

Tracert检测可以查看交换机到目标节点所经过的路由器。当网络出现故障时，使用该命令可以分析出现故障的网络节点。

在IP数据包首部中包含一个TTL字段，当数据包在网络中转发时，每经过一个路由TTL字段的值减1。当接收的IP数据包的TTL字段为0或1时，路由器将此数据包丢弃，并给发送源回复一个ICMP超时报文。这样能有效防止数据包在网络发生故障时，无休止地在网络中流动。

Tracert检测过程如下：

1) 交换机发送一个TTL为1的报文给目的设备；
2) 第一跳（即该报文所到达的第一个路由器）回应一个TTL超时的ICMP报文（该报文中含有第一跳的IP地址），这样交换机就得到了第一个路由器的地址；
3) 交换机重新发送一个TTL为2的报文给目的设备；
4) 第二跳回应一个TTL超时的ICMP报文，这样交换机就得到了第二个路由器的地址；
5) 重复以上过程直到最终到达目的设备，交换机就得到了从它到目的设备所经过的所有路由器的地址。

进入页面的方法：系统维护>>网络诊断>>Tracert检测

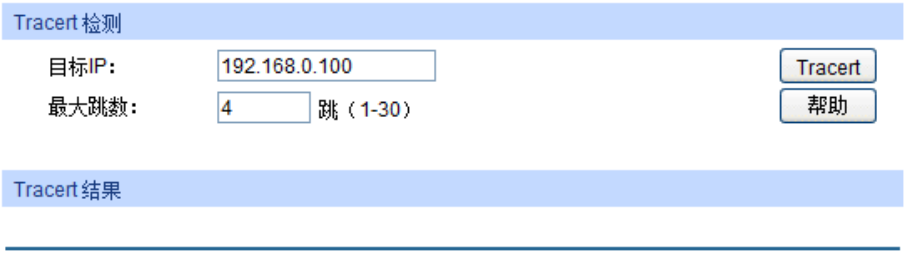


图 18-10 Tracert检测

条目介绍：

- **Tracert检测**

目标IP： 填写目的设备的IP地址。

最大跳数： 填写测试报文发送的最大跳数。

回目录

第19章　软件系统维护

在本交换机中，可以通过FTP功能加载软件。FTP（File Transfer Protocol，文件传输协议）在TCP/IP协议族中属于应用层协议，主要用于在远端服务器和本地主机之间传输文件，是IP网络上传输文件的通用协议。当交换机软件出故障导致无法正常启动时，也可以采用FTP功能重新加载软件。

19.1　硬件连接图

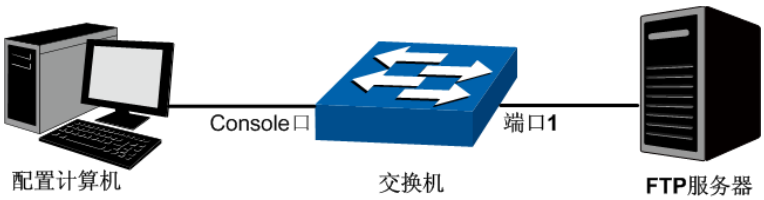


图 19-1 利用FTP加载软件连接图

1. FTP服务器通过端口1连接到交换机。
2. 配置计算机通过Console口与交换机连接。配置计算机和FTP服务器可以是同一台主机。
3. 将交换机软件存储在FTP服务器的共享目录下，并记录相应用户名、密码以及交换机软件名称，以便后续使用。

19.2　配置超级终端

完成硬件连接后，请按照下面步骤配置管理计算机的超级终端，以便管理交换机。

1. 选择**开始>>所有程序>>附件>>通讯>>超级终端**，打开超级终端。

图 19-2 打开超级终端

2. 弹出如图 19-3所示的连接描述窗口，在名称处键入一个名称，点击**确定**。

图 19-3 连接描述

3. 在图 19-4中选择连接串口，点击**确定**。

图 19-4 连接端口选择

4. 参考下图参数设置：每秒位数“38400”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，然后点击**确定**即可。

图 19-5 端口属性设置

19.3 bootUtil菜单下加载软件

利用FTP功能加载软件需要进入交换机的bootUtil菜单。请按照下面提示步骤进行操作：

1. 将配置计算机的串口连接到交换机的Console口，并打开配置成功的超级终端。FTP服务器连接到交换机端口1。

2. 将交换机断电重启，当在超级终端界面中看到提示信息Press CTRL-B to enter the bootUtil时，同时按下Ctrl按键和B字母按键进入bootUtil菜单，如图 19-6所示。

```
Press CTRL-B to enter the bootUtil
                ******************************************
                *          TPLINK  BOOTUTIL(v1.0.0)        *
                ******************************************
                Copyright (c) 2014 TPLINK
                Create Date: Jan 17 2014 11:24:43

   Boot Menu
0  - Print this boot menu
1  - Reboot
2  - Reset
3  - Start
4  - Start and ignore the configuration file
5  - Set ip address
6  - Select Startup Configuration file
7  - Activate Backup Image
8  - Download a configuration file
9  - Download a image file
10 - Delete a configuration file
11 - Delete the Backup Image file
12 - Update bootutil
13 - Display files
14 - Display image(s) info

Enter your choice(0-14)

[TPLINK]:
```

图 19-6 bootUtil菜单

由于该提示信息显示时间较短，可以在交换机上电后一直按住Ctrl按键和b字母按键不放，直到进入bootUtil菜单。

3. 进入bootUtil菜单后，首先配置交换机的IP参数。IP参数配置接口为5，此处设置交换机的IP地址为10.10.70.22，掩码为255.255.255.0，网关设置为10.10.70.1。详细命令设置如下图所示。

```
[TPLINK]: 5
  Ip Address (192.168.0.1):10.10.70.22
  Ip Mask (255.255.255.0):
  Gateway (192.168.0.1):10.10.70.1
Init network....
Init network done
```

4. 然后配置存放升级软件的FTP服务器的参数以及镜像文件名称，并将镜像文件重命名，通常如果下载镜像要作为启动镜像，则重命名为image1.bin；如果下载镜像要作为备份镜像，则重命名为image2.bin。FTP服务器参数设置接口为9，此处假设FTP服务器IP地址为10.10.70.146，

登录FTP服务器的用户名为3700和密码均为123，镜像名称为image.bin，并重命名为镜像文件名称为image1.bin。详细命令如下图所示。

```
[TPLINK]: 9
1 - get the image file by ftp
2 - get the image file by xmodem
0 - return
Enter your choice (0-2):1
  Ftp Ip Address (192.168.0.146):10.10.70.146
  Ftp user (3700):
  Ftp password (123):
  Ftp fileName (*.bin):image.bin
You can only use the port 1 to download file
Received a file by ftp in 19s. Size is 5361248 bytes
Specify the image name in system:
1 - image1.bin
2 - image2.bin
0 - cancel and return
Enter your choice (0-2):1
.................................................
```

5. 成功下载镜像后，需要将镜像文件设置为启动镜像或备份镜像，如下图所示。

```
Specify the attribute of the image file(image1.bin):
1 - Startup Image
2 - Backup Image
0 - use default
Enter your choice (0-2):1
Parsing image1.bin...
Parsing image done
Set image1.bin as the Startup Image...
```

6. 当超级终端弹出前导符[TP-LINK]时，表示通过FTP下载镜像文件已经完成，此时可以输入1正常启动交换机，如下图所示。

```
[TPLINK]: 1
Are you sure to reboot the device?[Y/N]:y
 Rebooting...

POST:Memory Tests:Begin
POST:Memory Tests:End,Status Passed
POST:Flash Tests:Begin
POST:Flash Tests:End,Status Passed
POST:File System Tests: Begin
POST:File System Tests: End,Status Passed
POST:CMIC Registers Tests: Begin
POST:CMIC Registers Tests: End,Status Passed
POST:MAC And PHY Registers Tests: Begin
POST:MAC And PHY Registers Tests: End,Status Passed
POST:Fan Tests: Begin
POST:Fan Tests: End,Status Passed
POST:RPS Tests: Begin
POST:RPS Tests: End,Status Passed
POST:MCard Tests: Begin
POST:MCard Tests: End,Status Passed

Press CTRL-B to enter the bootUtil
Get Operational Code from Startup Image...
Parsing image1.bin...
Parsing image is done
Start to init Flash...
Start to init the configuration of the image...
Init the configuration of the image done
Init Flash done
Decompressing T3700_2014-01-15 .img in image1.bin...
Starting...



T3700G-28TQ>
```

当出现机型前导符T3700G-28TQ>时表示已完成启动，可以通过命令行管理交换机。

7. 当忘记了登录交换机的用户名和密码时，可在第2步进入交换机bootUtil菜单后输入2进行软件复位，复位后配置参数恢复到出厂状态，交换机的登录用户名和密码均为admin。

回目录

附录A 802.1X客户端软件使用说明

在802.1X体系结构中，客户端作为接入设备需要安装相应的客户端软件，且软件遵循802.1X协议标准才能够顺利通过认证。当使用本交换机进行认证时，请使用我司提供的客户端软件进行认证。

1. 安装说明

1. 将光盘放入计算机光驱，在光盘文件夹中，双击安装软件图标  ，弹出安装语言选择对话框，如下图1所示。

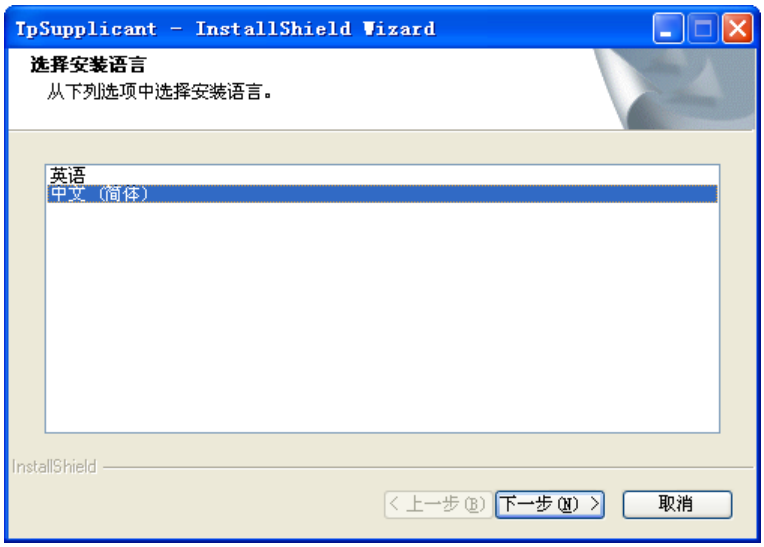


图1 选择安装语言对话框

2. 单击下一步进入安装准备过程，如下图2所示：

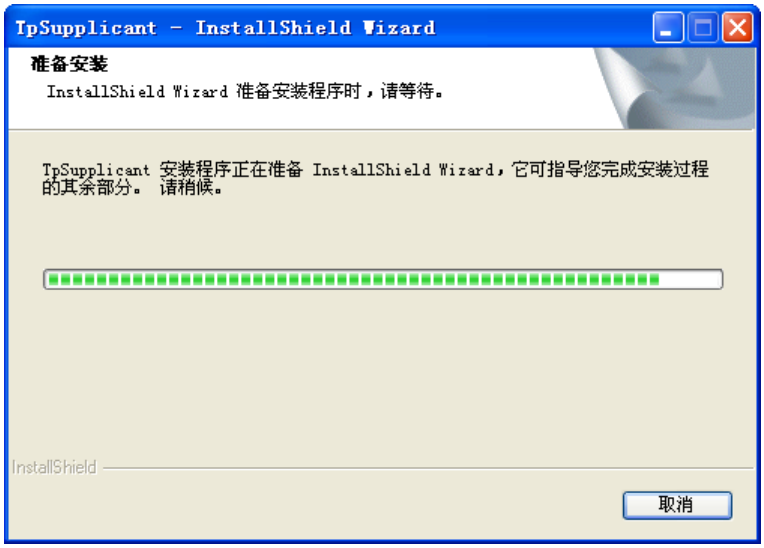


图2 准备安装对话框

3. 等待片刻，系统准备工作完成后，将自动弹出欢迎对话框，如下图3所示，此时可点击<取消>终止安装过程：

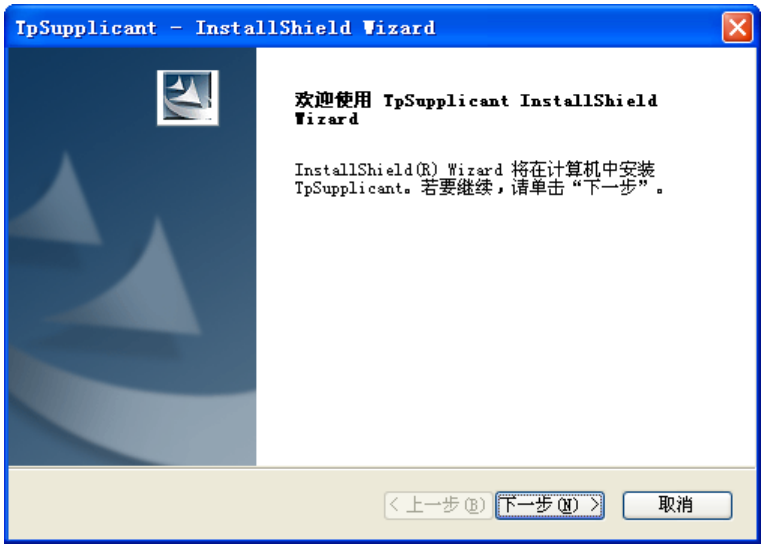


图3 欢迎对话框

4. 点击<下一步>进行安装路径的选择，如下图4所示。点击<更改...>可以选择合适的安装路径。

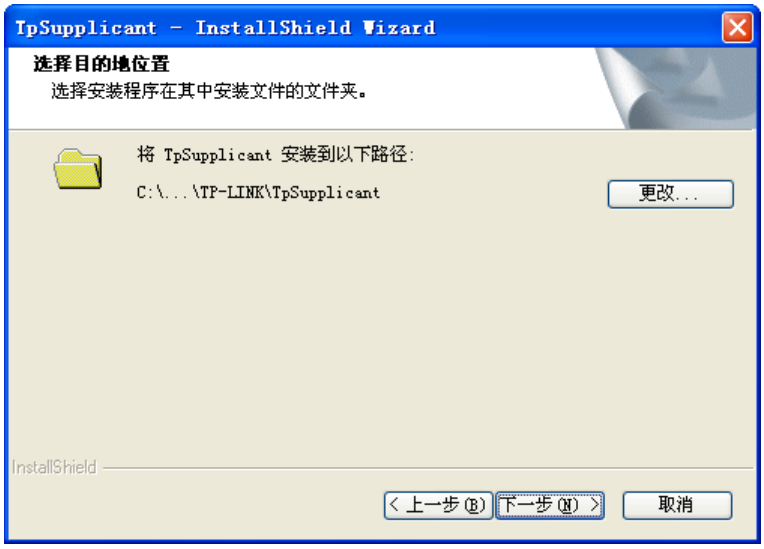


图4 安装路径对话框

5. 至此，安装所需参数已确定。点击<下一步>，弹出安装对话框。如下图5所示：

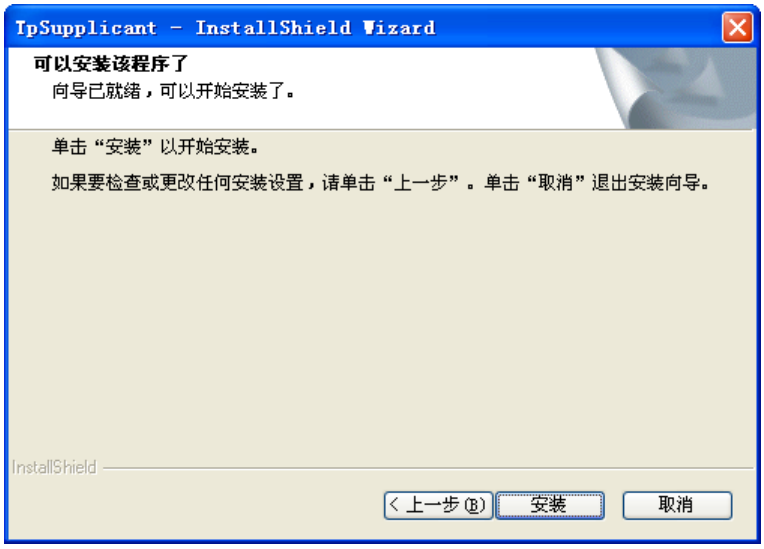


图5 正在安装

6. 点击<安装>，开始安装802.1X客户端软件，如下图6所示：

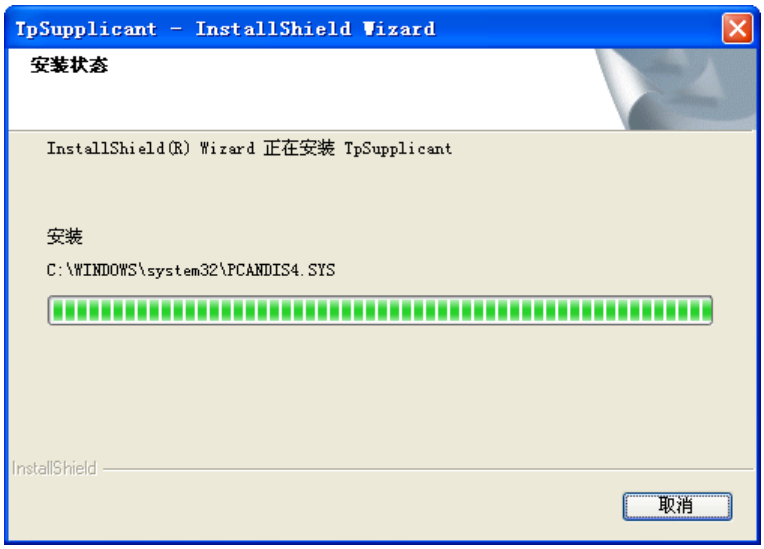


图6 安装过程

7. 等待片刻，将弹出安装完成对话框。如下图7所示：

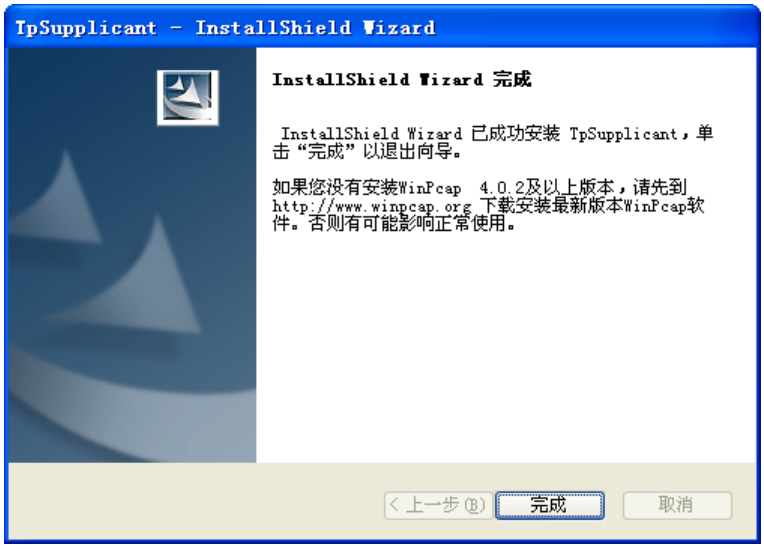


图7 安装完成对话框

8. 根据页面提示，安装完成后，如果计算机上没有安装WinPcap 4.0.2版本以上的软件，将无法使用该802.1X客户端进行认证。请在网上下载WinPcap软件并安装。点击<完成>退出。

2. 卸载说明

当需要卸载TpSupplicant软件时，可以按照下面步骤执行：

1. 选择：**开始 >> 所有程序 >> TP-LINK >> TpSupplicant >> 卸载802.1X客户端**进行客户端软件卸载。软件卸载准备对话框如下图8所示：

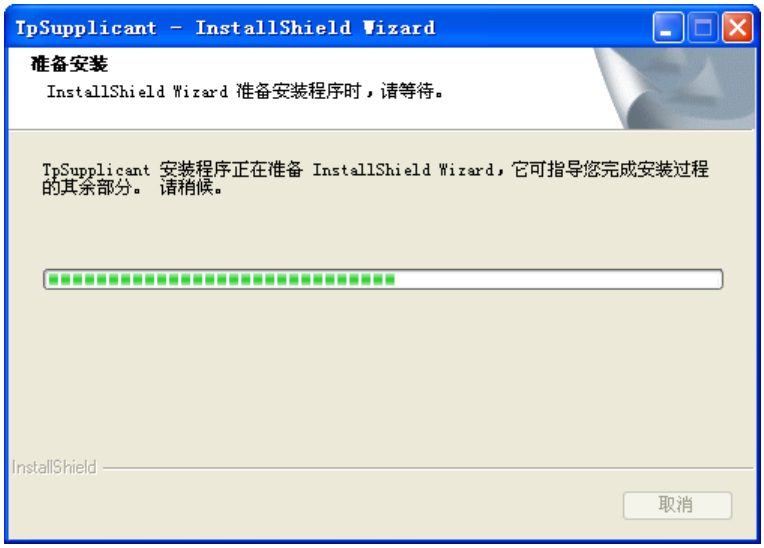


图8 软件卸载准备

2. 点击<是>，开始卸载软件，如下图9所示：

图9 卸载软件

3. 卸载结束后，点击<完成>关闭窗口即可，如下图10所示：

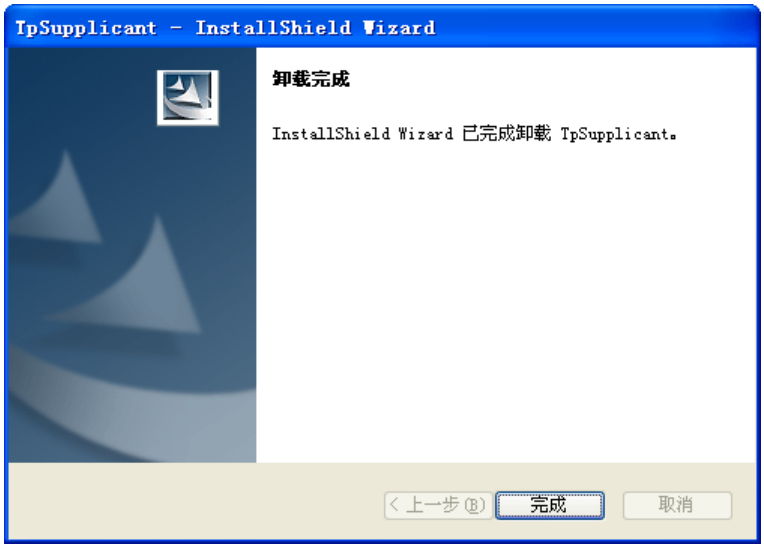


图10 完成卸载

3. 使用说明

1. 安装完成后，双击桌面**TP-LINK** 802.1X客户端软件图标运行应用程序，弹出程序主对话框如下图11所示：

图11 主对话框

在用户名和密码中输入服务器端设定好的用户名和密码，注意用户名和密码均不得多于16个字符。

2. 点击<属性>按键，弹出属性对话框，可以对拨号属性进行适当的设置，如下图12所示：

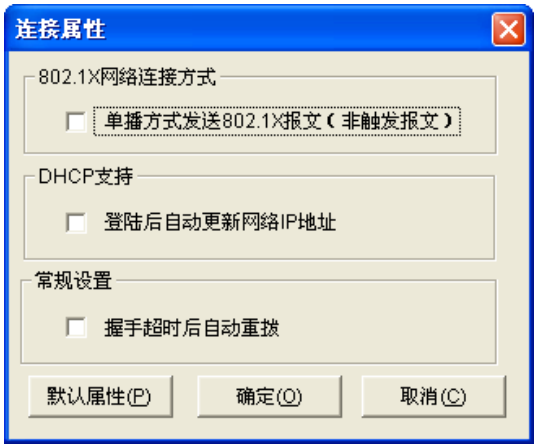


图12 属性对话框

单播方式发送802.1X报文（非触发报文）：选择此项时，客户端将以组播的方式向交换机申请认证，然后以单播方式发送认证报文。

登陆后自动更新IP地址：如果接入网络中设置了DHCP服务器为客户端分配IP，请选择此项功能。认证成功后DHCP服务器会自动给客户端分配IP地址，客户端获得新的IP地址后才能访问网络。

握手超时后自动重拨：选择此项时，如果客户端在一定的时间内没有收到交换机的握手应答报文，则说明客户端和交换机的连接可能出现问题，这时客户端软件将自动重新发起连接。

3. 在主窗口如图11界面下如果点击<连接>，将弹出认证状态对话框显示认证过程，如下图13所示：

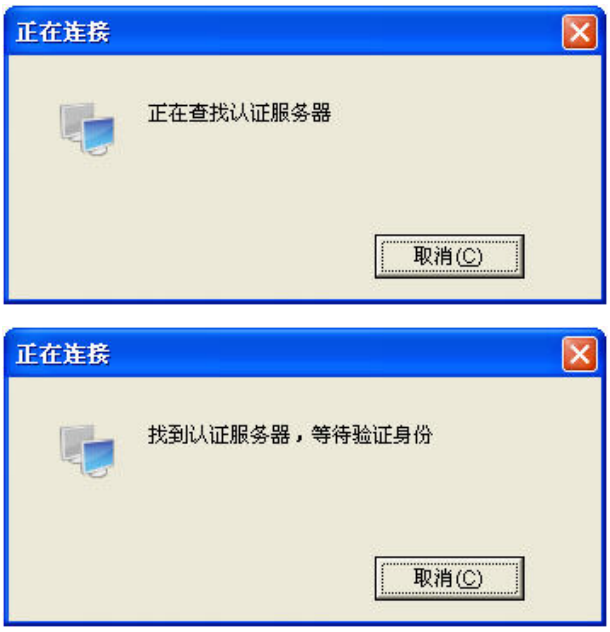


图13 认证状态对话框

4. 当顺利的通过认证后，会显示一个认证通过对话框，如下图14所示：

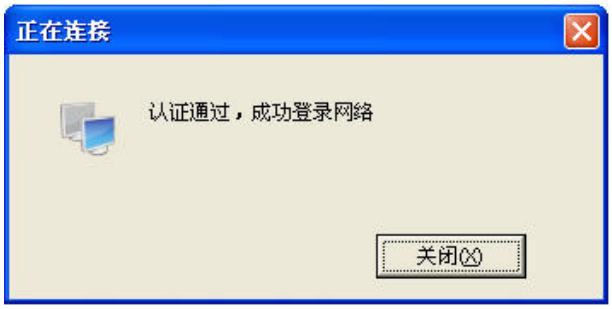


图14 认证通过对话框

5. 双击系统托盘中的连接状态图标，将弹出连接状态对话框，如下图15所示：

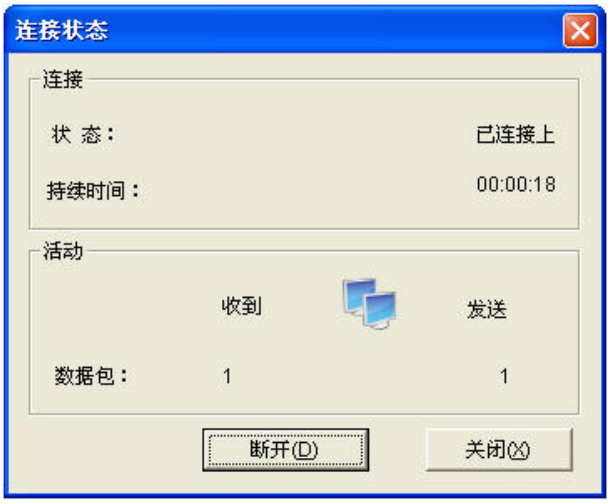


图15 连接状态对话框

4. 常见问题：

1. 当我运行该软件的时候为什么会出现如下图所示的错误对话框？

图16 缺失DLL对话框

答：如果出现图16对话框，说明缺少了支持的DLL文件，如果没有安装WinPcap 4.0.2或以上版本，请先到http://www.winpcap.org下载安装最新版本WinPcap软件，然后重新运行该客户端。

2. 可以使用该软件拨号其它公司生产的交换机吗？

答：不可以，该软件是专门为我司交换机定制。

3. 如果我设置保存密码会不会不安全？

答：不会，保存到配置文件中的密码已经经过加密。

回目录

附录B 术语表

【 # A B C D E F G H I J L M N O P Q R S T U V W 】

英文缩写	英文全称	中文全称
A		回首页
AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
-	Auto-Negotiation	自协商
B		回首页
BOOTP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
-	Broadcast Storm	广播风暴
-	Broadcast	广播
-	Broadcast Domain	广播域
C		回首页
CFI	Canonical Format Indicator	标准格式指示位
CHAP	Challenge Handshake Authentication Protocol	质询握手验证协议
CIST	Common and Internal Spanning Tree	公共和内部生成树
CMP	Cluster Management Protocol	集群管理协议
CRC	Cyclic Redundancy Check	循环冗余校验
CoS	Class of Service	服务等级
CSMA/CD	Carrier Sense Multiple Access/Collision Detect	载波侦听多路访问/冲突检测
CST	Common Spanning Tree	公共生成树
D		回首页
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
-	DHCP Client	DHCP客户端
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
DSCP	Differentiated Services Code Point	差分服务编码点
E		回首页
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPOL	Extensible Authentication Protocol over LAN	局域网上的可扩展认证协议
EAPOR	EAP over RADIUS	承载于RADIUS协议的EAP
-	Ethernet	以太网

英文缩写	英文全称	中文全称
F		回首页
FE	Fast Ethernet	快速以太网
FDB	Forward Data Base	地址表
-	Flow Control	流控
-	Frame	帧
FTP	File Transfer Protocol	文件传输协议
-	Full-Duplex	全双工
G		回首页
GARP	General Attributes Registration Protocol	通用属性注册协议
GBIC	Giga Bitrate Interface Converter	千兆接口转换器
GE	Gigabit Ethernet	千兆以太网
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
H		回首页
-	Half-Duplex	半双工
HTTP	Hyper Text Transport Protocol	超级文本传送协议
HTTPS	Secure Hyper Text Transfer Protocol	安全超文本传输协议
I		回首页
IANA	Internet Assigned Numbers Authority	因特网编号授权委员会
ICMP	Internet Control Message Protocol	因特网控制报文协议
IEEE	Institute of Electrical and Electronics Engineers	电机工程师协会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	互联网组管理协议
-	IGMP-Snooping	互联网组管理协议窥探
IP	Internet Protocol	互联网协议、网际协议
-	IP Address	IP地址
-	IP Multicast	IP组播
ISO	International Organization for Standardization	国际标准化组织
ISP	Internet service provider	因特网服务提供商
IST	Internal Spanning Tree	内部生成树
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	国际电信联盟-电信标准部
J		回首页
-	Jumbo Frame	超长帧
L		回首页
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议

英文缩写	英文全称	中文全称
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAG	Link Aggregated Group	链路聚合组
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
M		回首页
MAC	Media Access Control	媒体访问控制
MAPT	Network Address Port Translation	网络地址端口转换
MIB	Management Information Base	管理信息库
MODEM	MOdulator-DEModulator	调制解调器
MSTI	Multi-Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTU	Maximum Transmission Unit	最大传输单元
-	Multicast	组播
N		回首页
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Net Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NMS	Network Management Station	网络管理站
NPDU	Network Protocol Data Unit	网络协议数据单元
NTDP	Neighbor Topology Discovery Protocol	邻居拓扑发现协议
NTP	Network Time Protocol	网络时间协议
-	NTP Server	网络时间服务器
O		回首页
OID	Object Identifier	对象标识符
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
OUI	Organizationally Unique Identifier	全球统一标识符
P		回首页
P2P	Point To Point	点到点
-	Packet	数据包
PAP	Password Authentication Protocol	密码认证协议
PCB	Printed Circuit Board	印制电路板
PDU	Protocol Data Unit	协议数据单元
PING	Packet Internet Groper	Internet包探测器
PoE	Power over Ethernet	以太网供电

英文缩写	英文全称	中文全称
-	Port	端口
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point to Point Tunneling Protocol	点对点隧道协议
PQ	Priority Queuing	优先队列
Q		回首页
QoS	Quality of Service	服务质量
-	Query	查询
R		回首页
RADIUS	Remote Authentication Dial in User Service	远程认证拨号用户服务
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Monitoring	远程网络监视
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
-	Router	路由器
S		回首页
-	Server	服务器
SFTP	Secure FTP	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SP	Strict Priority Queuing	严格优先级队列
SPF	Shortest Path First	最短路径优先
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	加密套接字协议层
STP	Spanning Tree Protocol	生成树协议
-	Switch	交换机
T		回首页
TCP	Transmission Control Protocol	传输控制协议
-	Telnet	远程登录
TFTP	Trivial File Transfer Protocol	简单文件传输协议
ToS	Type of Service	服务类型
TPID	Tag Protocol Identifier	标签协议标识符
TRIP	Trigger RIP	触发路由信息协议
TTL	Time to Live	生存时间
-	Trap	陷阱
U		回首页
UDP	User Datagram Protocol	用户数据包协议
-	Unicast	单播

英文缩写	英文全称	中文全称
URL	Uniform Resource Locators	统一资源定位
USM	User-Based Security Model	基于用户的安全模型
UTP	Unshielded Twisted Pair	非屏蔽双绞线
V		回首页
VACM	View-based Access Control Model	基于视图的访问控制模型
VLAN	Virtual Local Area Network	虚拟局域网
VOS	Virtual Operate System	虚拟操作系统
W		回首页
WAN	Wide Area Network	广域网
WLAN	wireless local area network	无线局域网
WRR	Weighted Round Robin Queuing	加权轮询队列
WWW	World Wide Web	万维网

回目录

附录C 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3i 10BASE-T以太网 IEEE 802.3u 100BASE-TX快速以太网 IEEE 802.3ab 1000BASE-T千兆以太网 IEEE 802.3z 1000BASE-X千兆以太网（光纤） IEEE 802.3ae 10GBASE-SR/LR 10G以太网（光纤） IEEE 802.3ad链路聚合 IEEE 802.3x流量控制 IEEE 802.1p优先级 IEEE 802.1q VLAN IEEE 802.1d STP生成树 IEEE 802.1s MSTP生成树 IEEE 802.1w RSTP生成树 ANSI/IEEE 802.3 N-Way自动协商 CSMA/CD Ethernet
数据传输速率	以太网 10Mbps半双工，20Mbps全双工 快速以太网 100Mbps半双工，200Mbps全双工 千兆以太网 2000Mbps全双工 10G以太网 20000Mpbs全双工
网络介质	10BASE-T： 3类或以上UTP/STP(≤100m) 100BASE-TX： 5类或以上UTP/STP(≤100m) 1000BASE-T： 4对超5类UTP/STP(≤100m) 1000BASE-X： 单模光纤或者多模光纤（可选） 10GBASE-SR： OM1/OM2/OM3或以上MMF（2m～300m） 10GBASE-LR： IEC的B1.1和B1.3的SMF（2m～10000m）
指示灯	Power, System, RPS, FAN, Master, Module, M1, M2, 10/100/1000Mbps, Unit ID数码指示灯
传输方式	存储转发
背板带宽	128Gbps
MAC地址学习	自动更新，支持32K地址空间
包转发速率	10BASE-T：14881pps/端口 100BASE-TX：148810pps/端口 1000BSAE-T：1488095pps/端口 1000BASE-X：1488095pps/端口 10GBASE-LR：14880952pps/端口

参数项	参数内容
交流输入	100-240V~ 50/60Hz
工作温度	0℃~40℃
存储温度	-40℃~70℃
工作湿度	10%~90%（RH 无凝结）
存储湿度	5%~90%（RH 无凝结）

回目录